CYBER FORENSICS

T.Y.B.Sc ComputerScience

(V Semester)
For Academic Year (2024-2025)

JNAN VIKAS MANDAL'S
PADMASHREE DR. R.T.DOSHI DEGREE COLLEGE OF INFORMATION TECHNOLOGY
MOHANLAL RAICHAND MEHTA COLLEGE OF COMMERCE DIWALIMAA DEGREE COLLEGE OF SCIENCE

CERTIFICATE

This is to certify that the Mr./Miss.________________________________of T.Y.B.Sc.(CS) Semester-V has completed the practical work in the subject of **CYBER FORENSICS** during the Academic year 2024-2025 under the guidance of **Mrs. Vinaya Mangnale.** being the partial requirement forthe fulfilment of the curriculum of Degree of Bachelor of Science in Computer Science, University of Mumbai.

Place: **Date:**

Sign of Subject Incharge Sign of External Examiner

Sign of In charge / H.O.D

INDEX

Practical 1

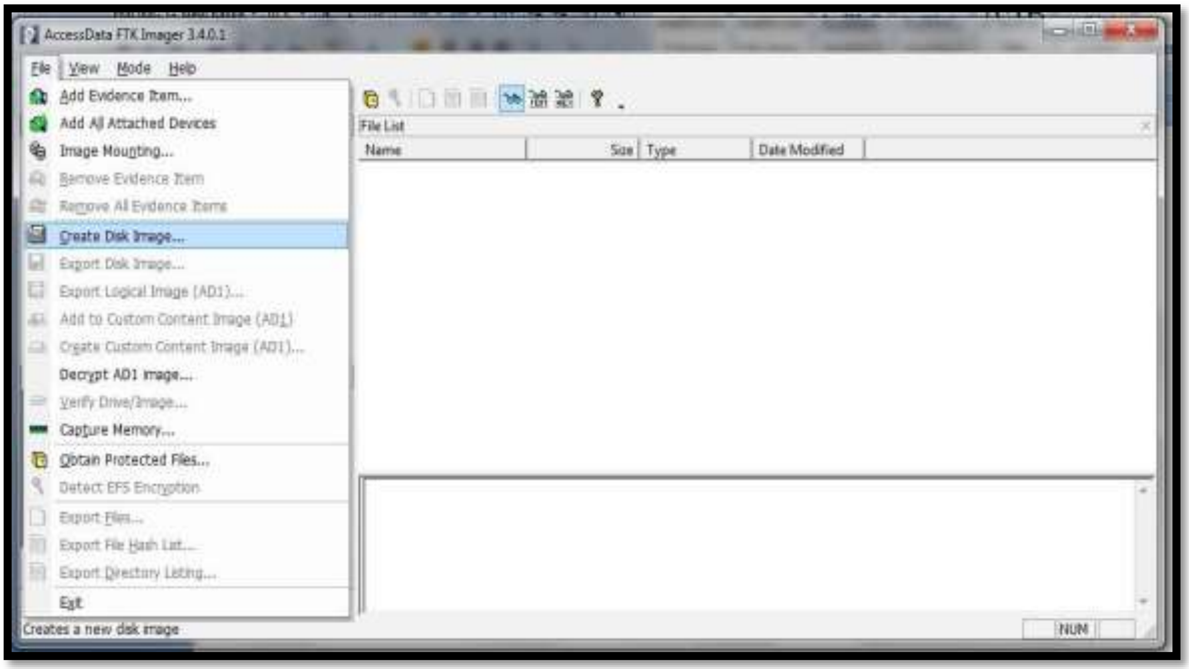
AIM: Creating a Forensic Image using FTK Imager.

Creating Forensic Image

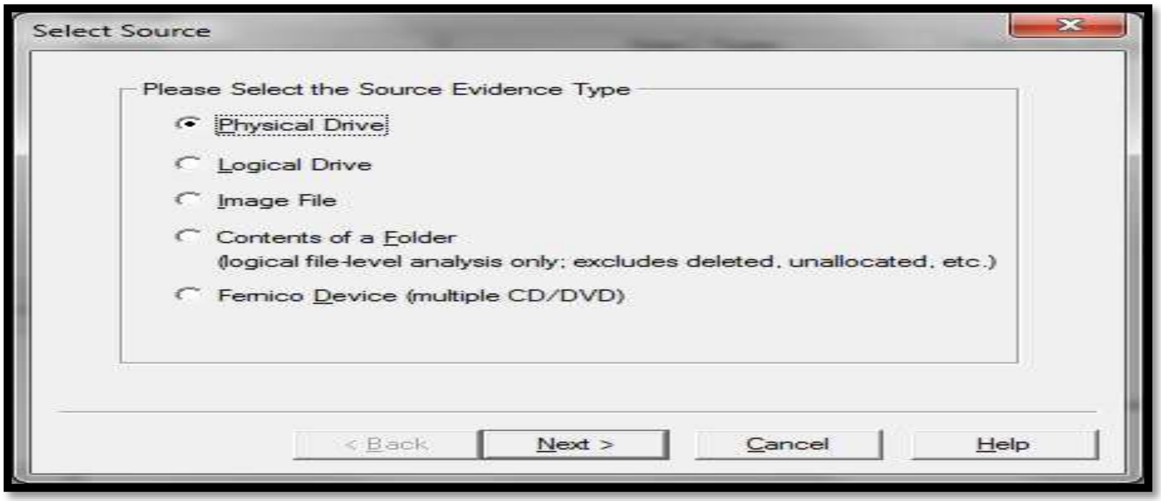
Check Integrity of Data

Analyze Forensic Image

Creating Forensic Images FTK
Imager allows you to write an image file to a single destination or to simultaneously write multiple image files to multiple destinations.
To create a forensic image:



1. **Click File, and then Create Disk Image, or click the button on the tool bar.**


Select Source

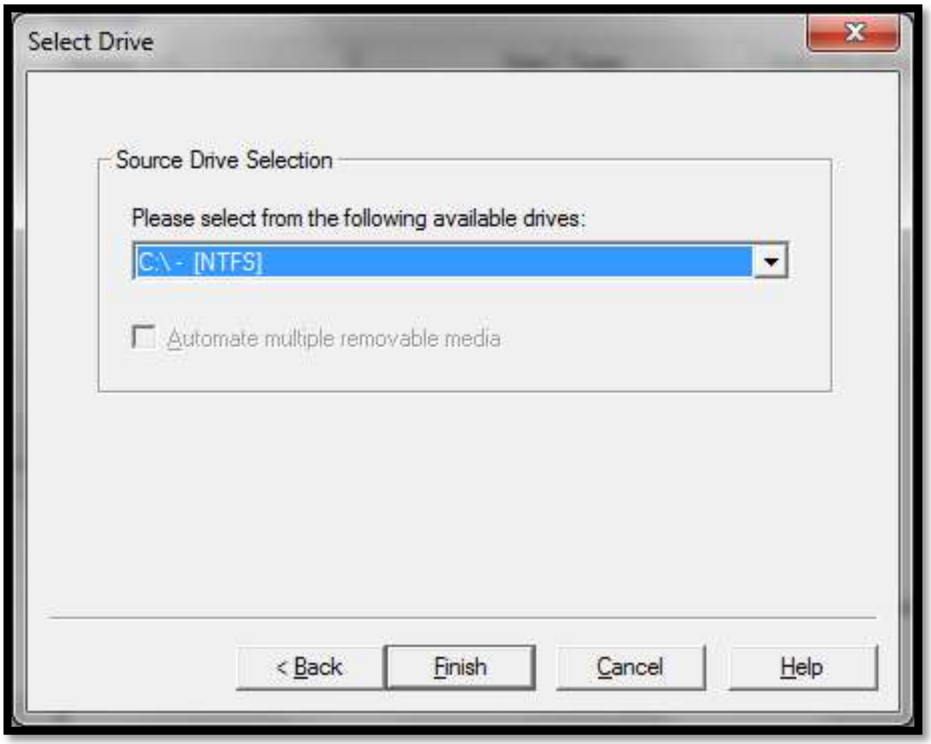
Please Select the Source Evidence Type

- ● Physical Drive
- ○ Logical Drive
- ○ Image File
- ○ Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)
- ○ Femico Device (multiple CD/DVD)

2. **Select the source you want to make an image of and click Next.**
   If you select Logical Drive to select a floppy or CD as a source, you can check the Automate multiple

removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

3. **Select the drive or browse to the source of the image you want, and then click Finish.**



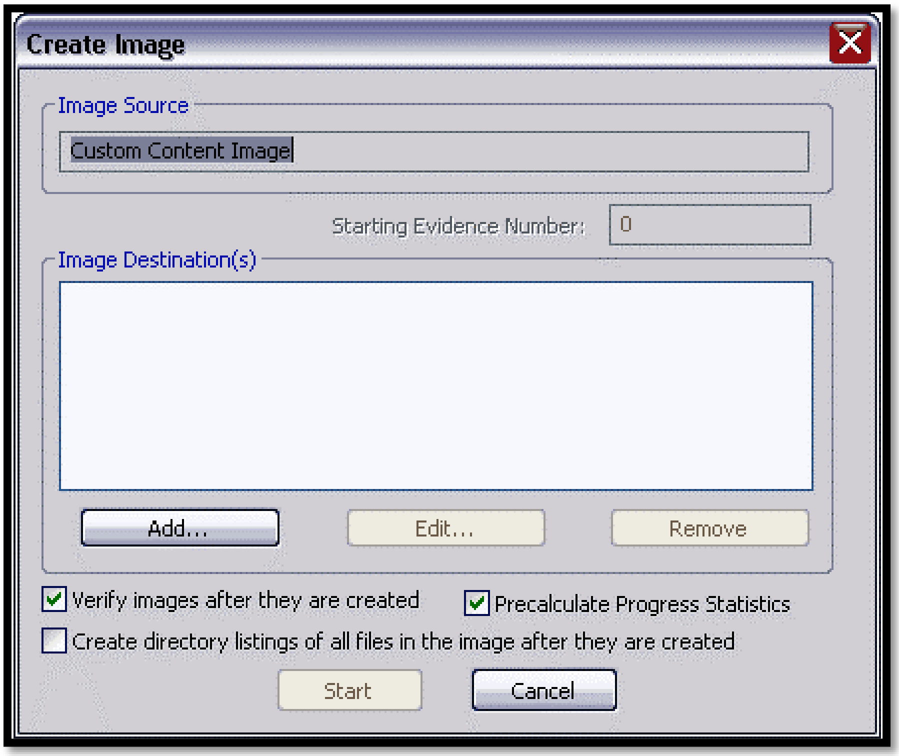
Select Drive

Source Drive Selection

Please select from the following available drives:

C:\ - [NTFS]

□ Automate multiple removable media



Create Image

Image Source

Custom Content Image

Starting Evidence Number: 0

Image Destination(s)

☑ Verify images after they are created ☑ Precalculate Progress Statistics

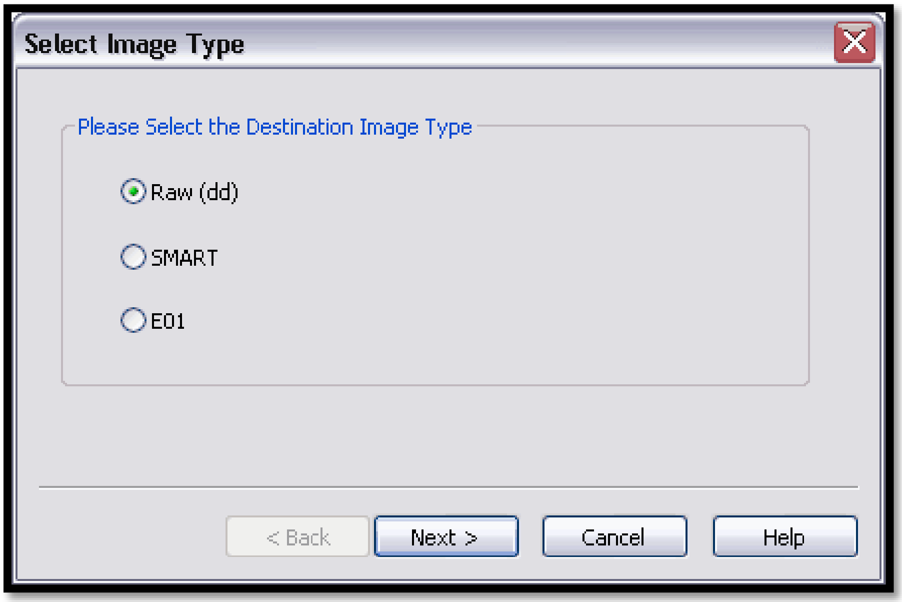
□ Create directory listings of all files in the image after they are created

4. **In the Create Image dialog, click Add.**

- You can compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn‟t have a hash, this option will generate one.

- You can list the entire contents of your images with path, creation dates, whether files were deleted and other metadata. The list is saved in a tab-separated value format

5. **Select the type of image you want to create, and then click Next.**
   Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format.



Select Image Type

Please Select the Destination Image Type

● Raw (dd)

○ SMART

○ E01

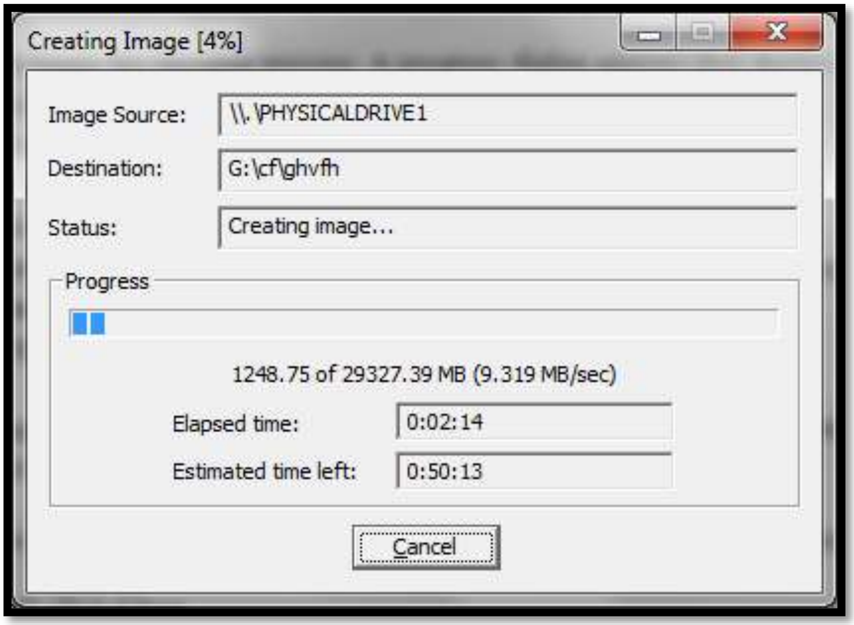
The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate space for the resulting image.
If you select SMART or E01 as the image type, complete the fields in the Evidence Item Information dialog, and click **Next**.
Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data).
SMART: This file format is designed for Linux file systems. This format keeps the disk images as pure bitstreams with optional compression. The file consists of a standard 13-byte header followed bya series of sections. Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if applicable.
E01: this format is a proprietary format developed by Guidance Software"s EnCase. This format compresses the image file. An image with this format starts with case information in the header and footer, which contains an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner"s name, special notes and an optional password.
AFF: Advance Forensic Format (AFF) was developed by Simson Garfinkel and Basis Technology. Its latest implementation is AFF4. The goal is to create a disk image format that does not lock the user into a proprietary format that may prevent them from being able to properly analyze it.

6. In the Image Destination Folder field, type the location path where you want to save the image file, or click **Browse** to find to the desired location.

   Note: If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location.

7. In the Image Filename field, specify a name for the image file but do not specify a file extension.
8. In the Image Fragment Size field, specify the maximum size in MB for each fragment of the image file. The s01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.
   Tip: If you want to transfer the image file to CD, accept the default fragment size of 650 MB.

9. Click **Finish**. You return to the Create Image dialog.
10. To add another image destination (i.e., a different saved location or image file type), click **Add**, and repeat steps 5– 10. To make changes to an image destination, select the destination you want to change and click **Edit.**
    To delete an image destination, select the destination and click **Remove**.
11. Click **Start** to begin the imaging process. Aprogress dialog appears that shows the following:
    - The source that is being imaged
    - The location where the image is being saved
    - The status of the imaging process
    - A graphical progress bar
    - The amount of data in MB that has been copied and the total amount to be copied
    - Elapsed time after the imaging process began



Creating Image [4%]

Image Source: \\.\PHYSICALDRIVE1

Destination: G:\cf\ghvfh

Status: Creating image...

Progress

1248.75 of 29327.39 MB (9.319 MB/sec)

Elapsed time: 0:02:14

Estimated time left: 0:50:13

    - Estimated time left until the process is complete
12. After the images are successfully created, click Image Summary to view detailed file information, including MD5 and SHA1 checksums.

Note: This option is available only if you created an image file of a physical or logical drive.

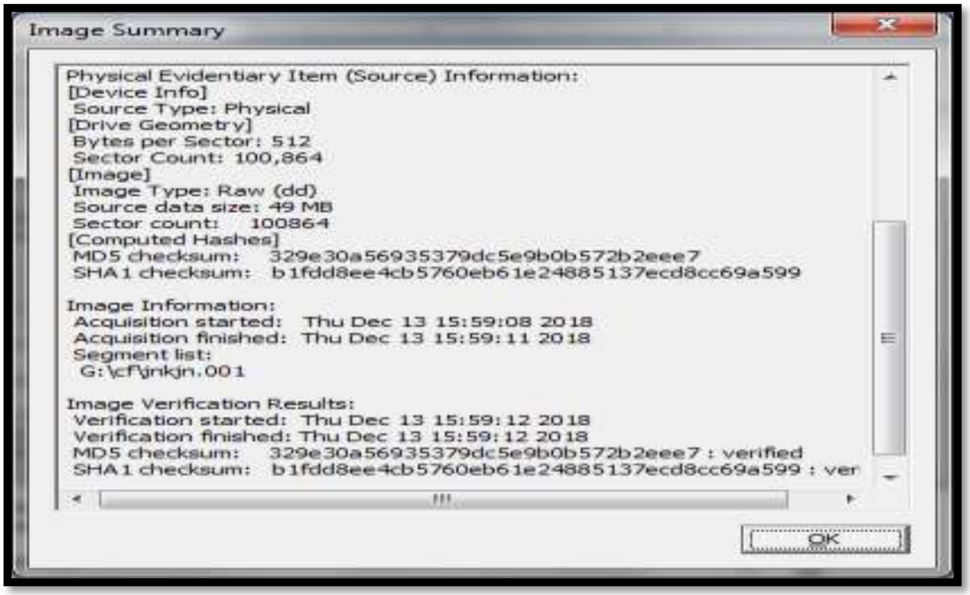


Image Summary

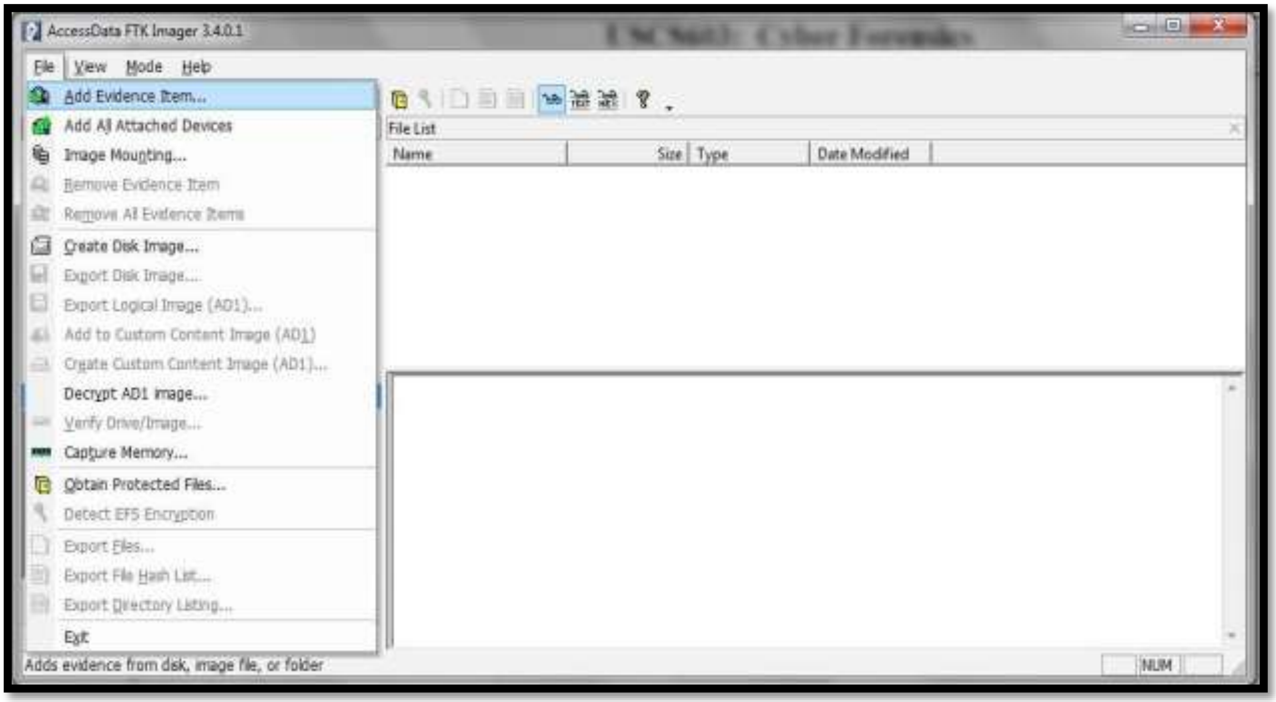
```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 100,864
[Image]
 Image Type: Raw (dd)
 Source data size: 49 MB
 Sector count:    100864
[Computed Hashes]
 MD5 checksum:    329e30a56935379dc5e9b0b572b2eee7
 SHA1 checksum:   b1fdd8ee4cb5760eb61e24885137ecd8cc69a599

Image Information:
 Acquisition started:  Thu Dec 13 15:59:08 2018
 Acquisition finished: Thu Dec 13 15:59:11 2018
 Segment list:
  G:\cf\jnkjn.001

Image Verification Results:
 Verification started:  Thu Dec 13 15:59:12 2018
 Verification finished: Thu Dec 13 15:59:12 2018
 MD5 checksum:    329e30a56935379dc5e9b0b572b2eee7 : verified
 SHA1 checksum:   b1fdd8ee4cb5760eb61e24885137ecd8cc69a599 : ver
```

13. When finished, click Close

Note that the image file (*.001) as well as the image summary file from above (*.txt) have been saved onto the „Drive". The .001 extension may be left as is, or can be changed to .dd. The .001 extension is used due to the fact that many times the file to be imaged is very large and must be split into multiple chunks. In that case, you would have *.001, *.002, etc.

Analyze Forensic Image:

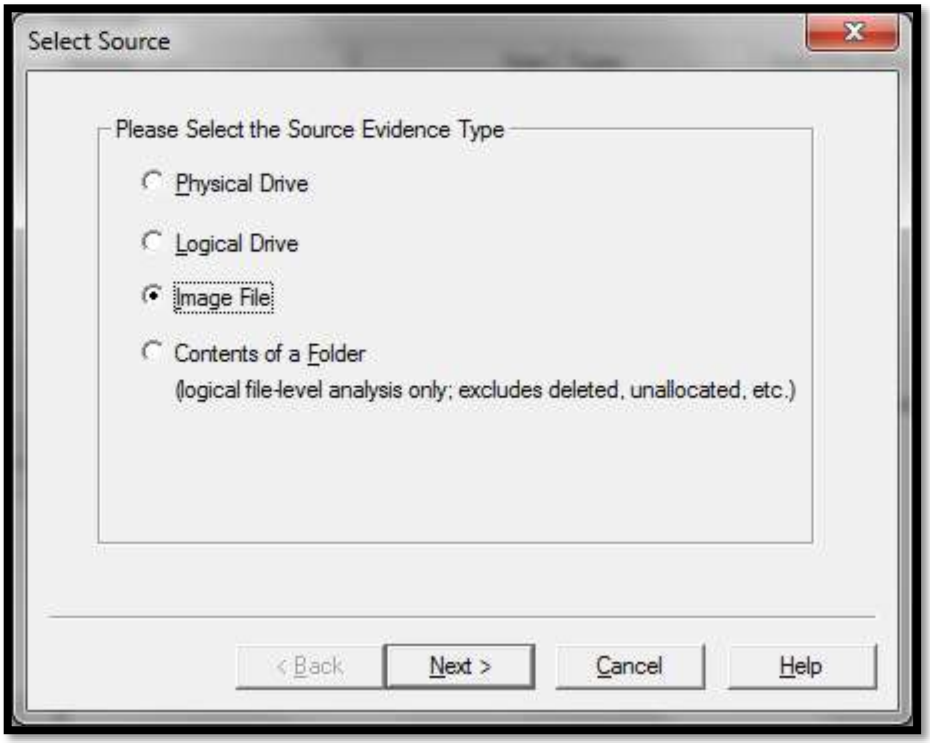
Click on Add Evidence Item to add evidence from disk, image file or folder.



AccessData FTK Imager 3.4.0.1

Adds evidence from disk, image file, or folder

Now select the source evidence type as physical drive, logical drive or image file. We have selected image file



Please Select the Source Evidence Type

○ Physical Drive

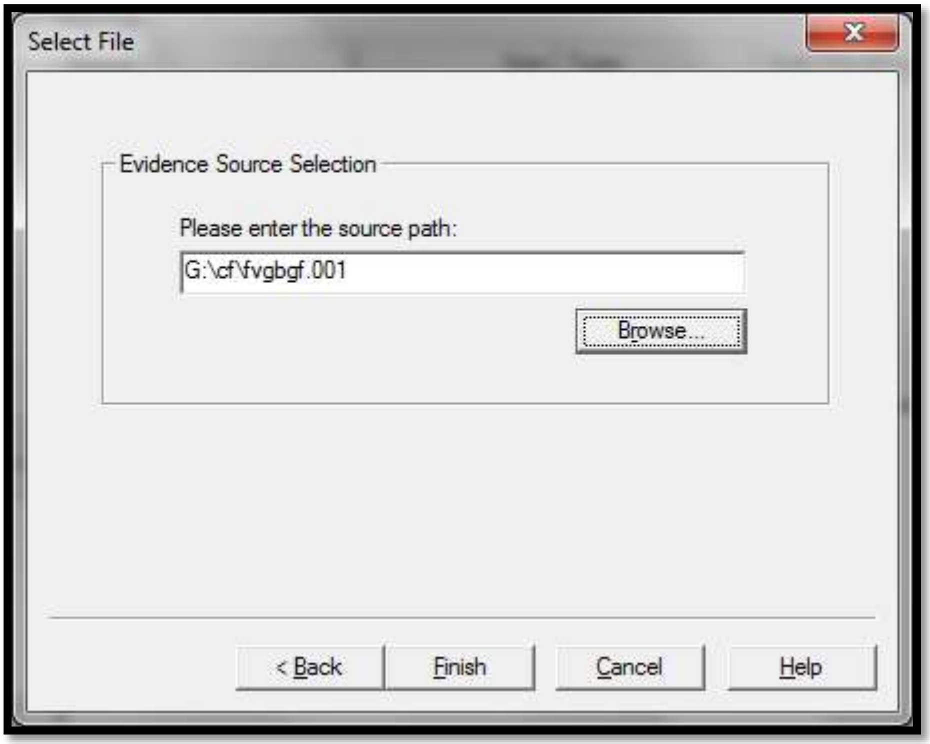
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

and click on next.

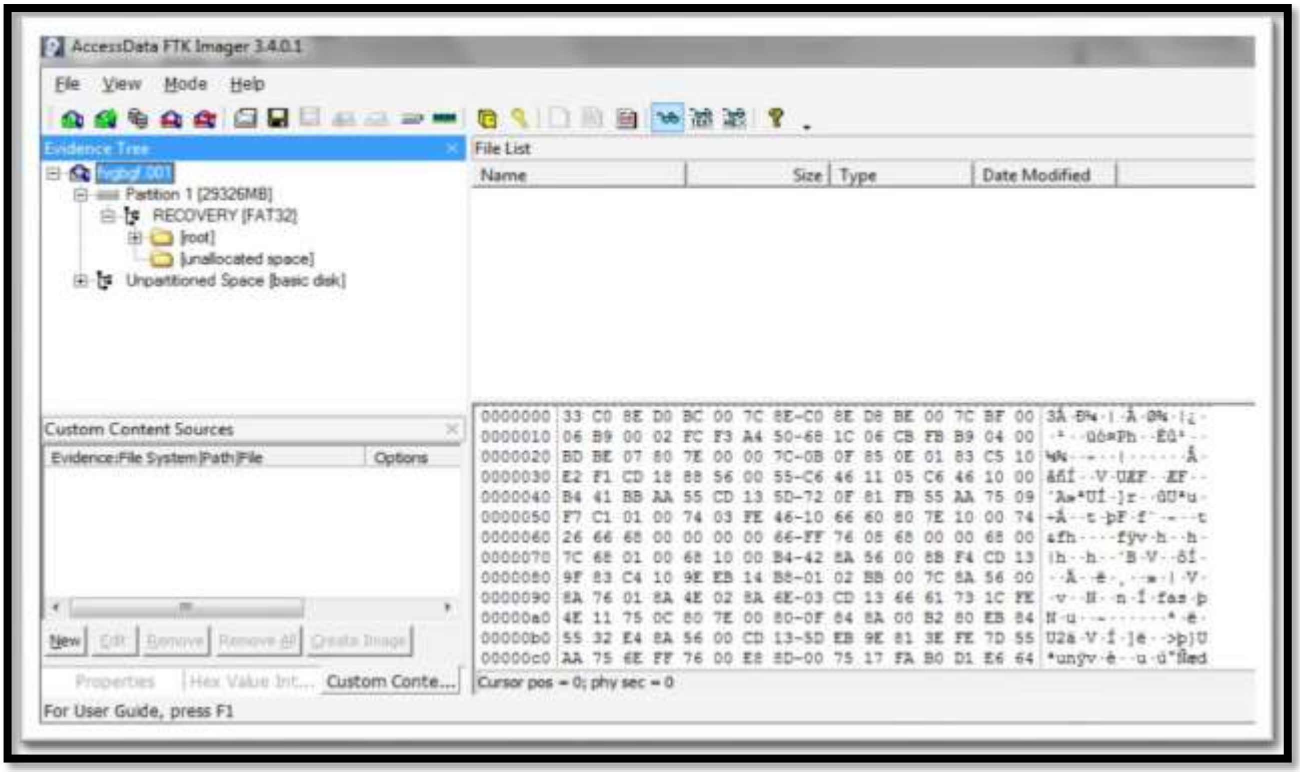
Select virtual drive image & click on open option.Select the source path and click on finish.



Evidence Source Selection

Please enter the source path: G:\cf\fvgbgf.001

Now select Evidence Tree and analyze the virtual disk as physical disk.



```
0000000 33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00 3À·Ð¼·|·À·Ø¾·|¿·
0000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00 ·¹··üó¤Ph··Ëû¹··
0000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10 ½¾··~··|······Å·
0000030 E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00 âñÍ··V·UÆF··ÆF··
0000040 B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 ´A»ªUÍ·]r··ûUªu·
0000050 F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74 ÷Á··t·þF·f`·~··t
0000060 26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00 &fh····fÿv·h··h·
0000070 7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13 |h··h··´B·V··ôÍ·
0000080 9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00 ··Ä··ë·¸··»·|·V·
0000090 8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE ·v··N··n·Í·fas·þ
00000a0 4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84 N·u··~······²·ë·
00000b0 55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55 U2ä·V·Í·]ë··>þ}U
00000c0 AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64 ªunÿv·è··u·ú°Ñæd
Cursor pos = 0; phy sec = 0
```

Similarly to add raw image select again add evidence item and click on image file and click on open option.

Click on finish.

Now raw image will be added as physical drive to analyze.

CONCLUSION:- We successfully created forensic image, checked integrity of that image and analyzed the image using FTK Toolkit.

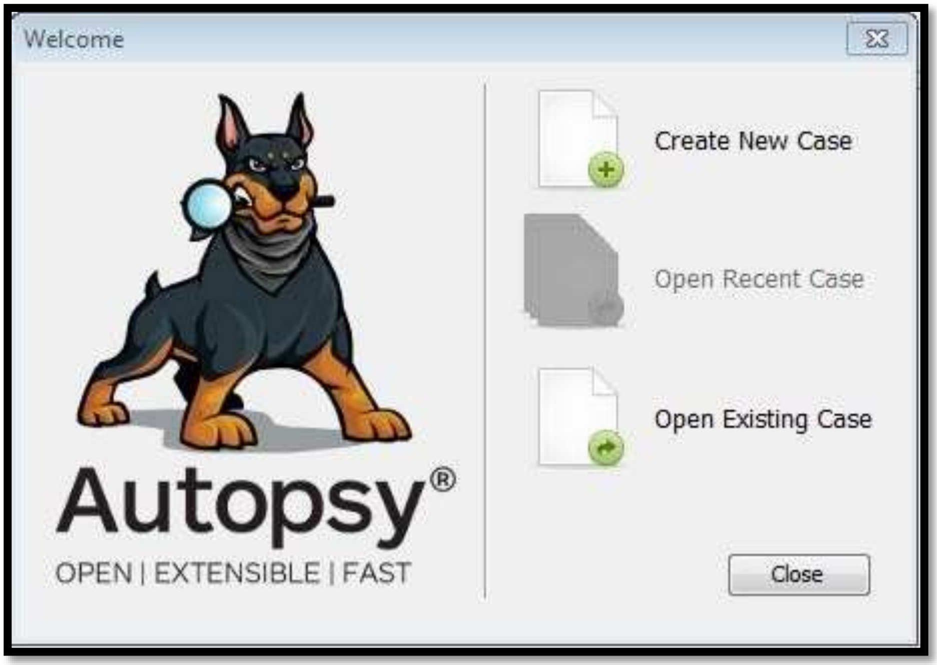
Practical 2

Data Acquisition

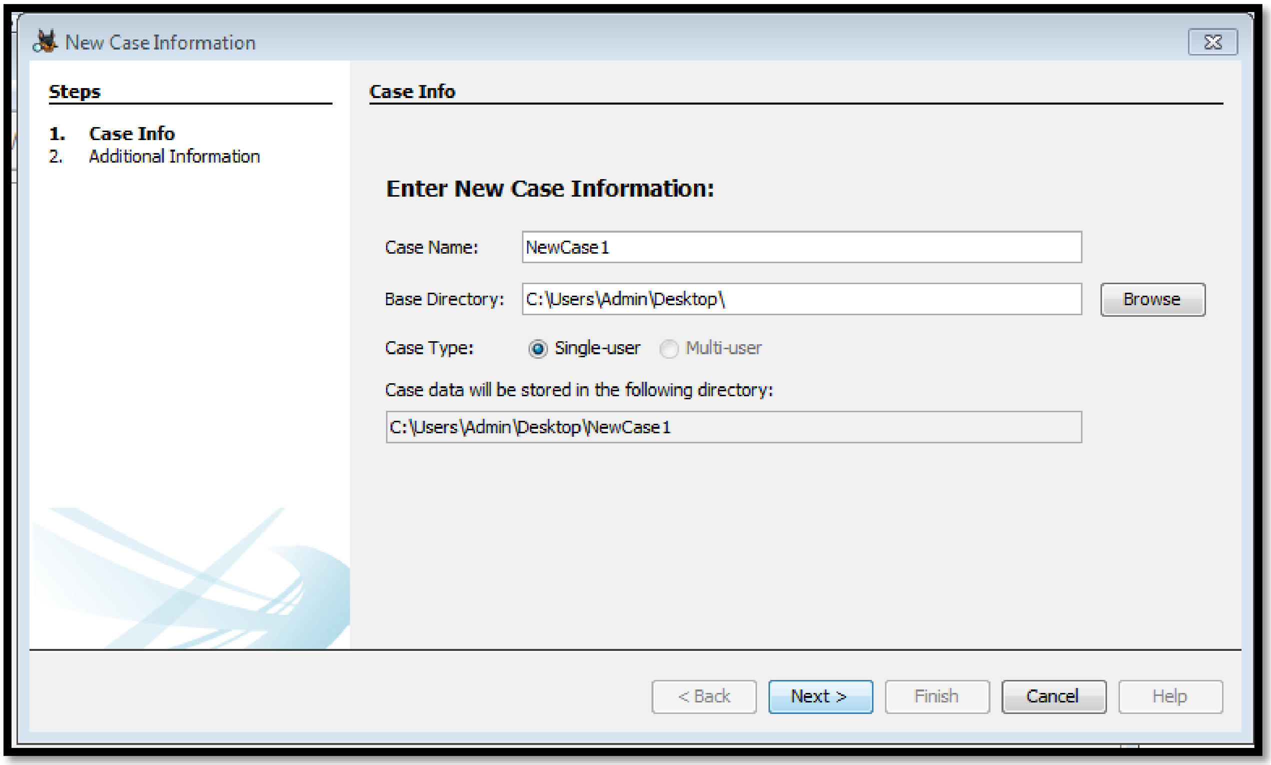
We are using Autopsy to solve the case study(image file).

Done loading modules.

1. Start Autopsy and Select “Create New Case”.



2. Enter Case Information.



Enter New Case Information:

Case Name: NewCase1

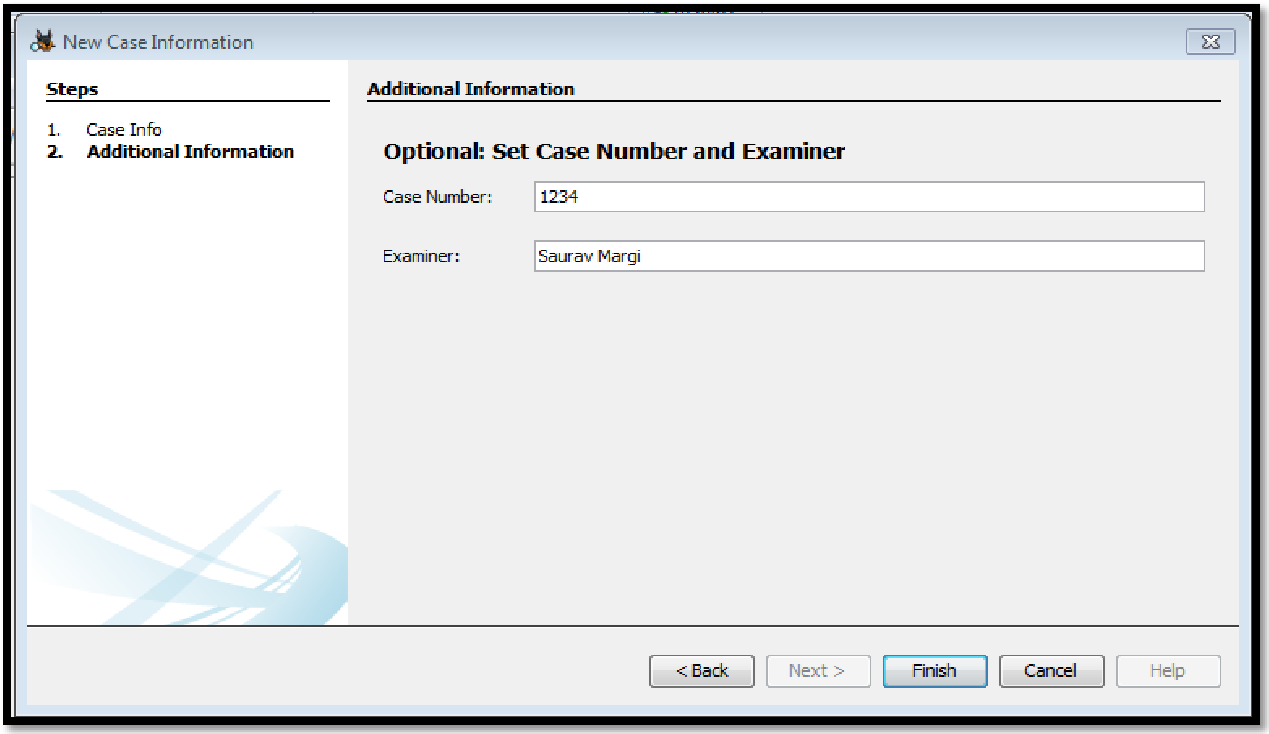
Base Directory: C:\Users\Admin\Desktop\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\Admin\Desktop\NewCase1

3. Enter Case Number and Examiner & Click Finish.

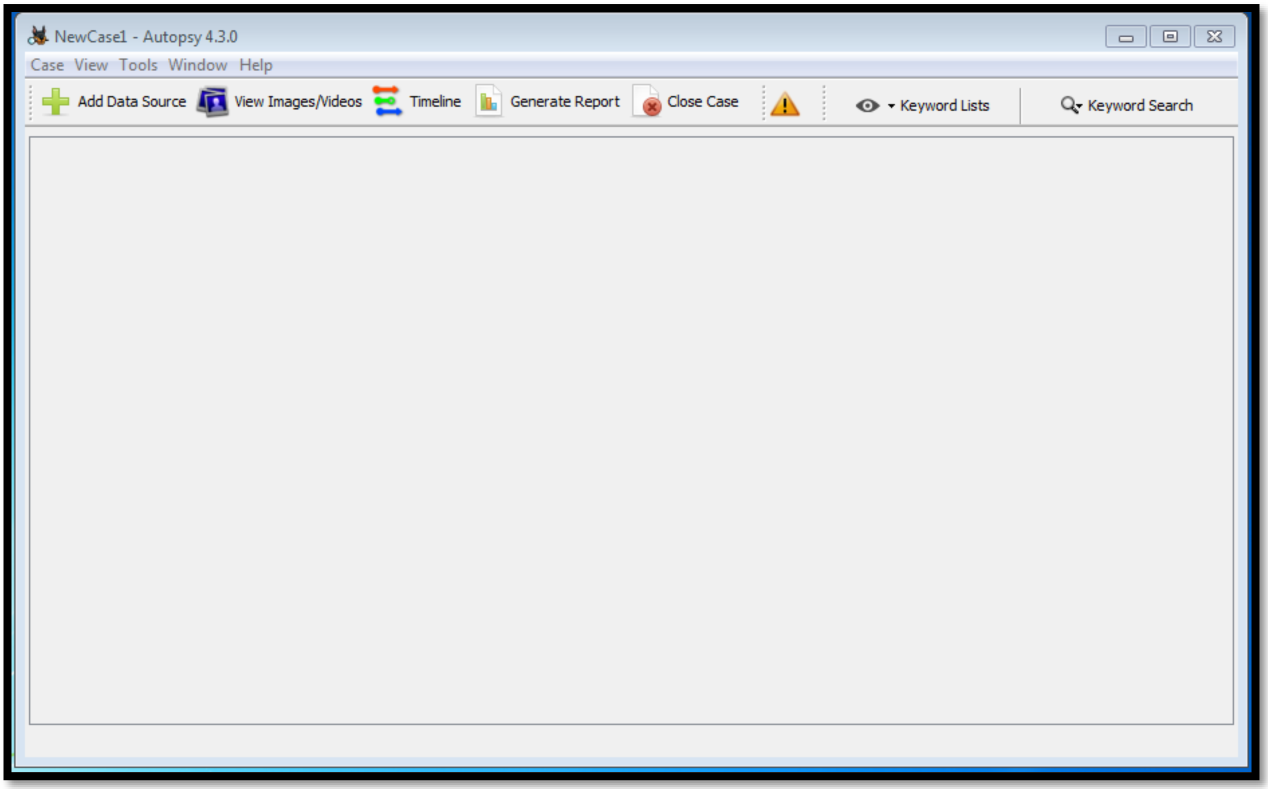


Optional: Set Case Number and Examiner

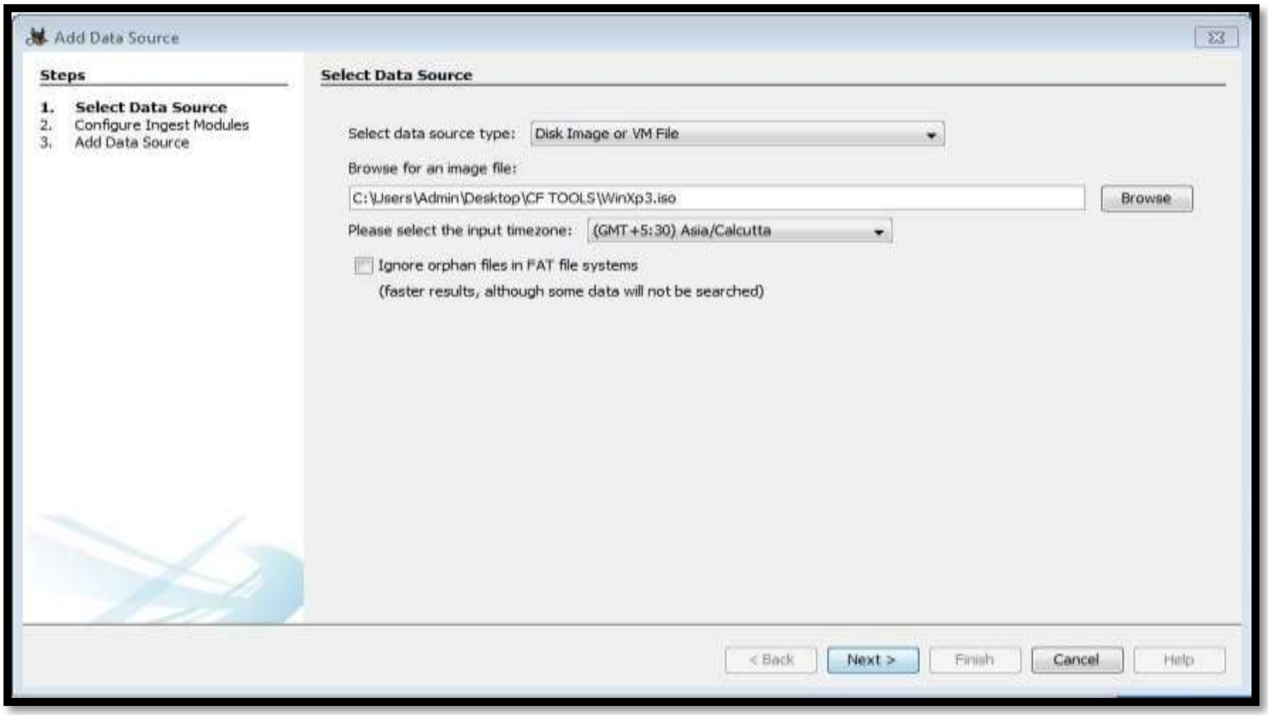
Case Number: 1234

Examiner: Saurav Margi

4. The case is created and displayed.



5. Add Data source details. Select data source type as Disk Image. Browse and select 'WinXp3.iso' file for an image file then Click 'Next'.



Steps

1. **Select Data Source**
2. Configure Ingest Modules
3. Add Data Source

Select Data Source

Select data source type: Disk Image or VM File

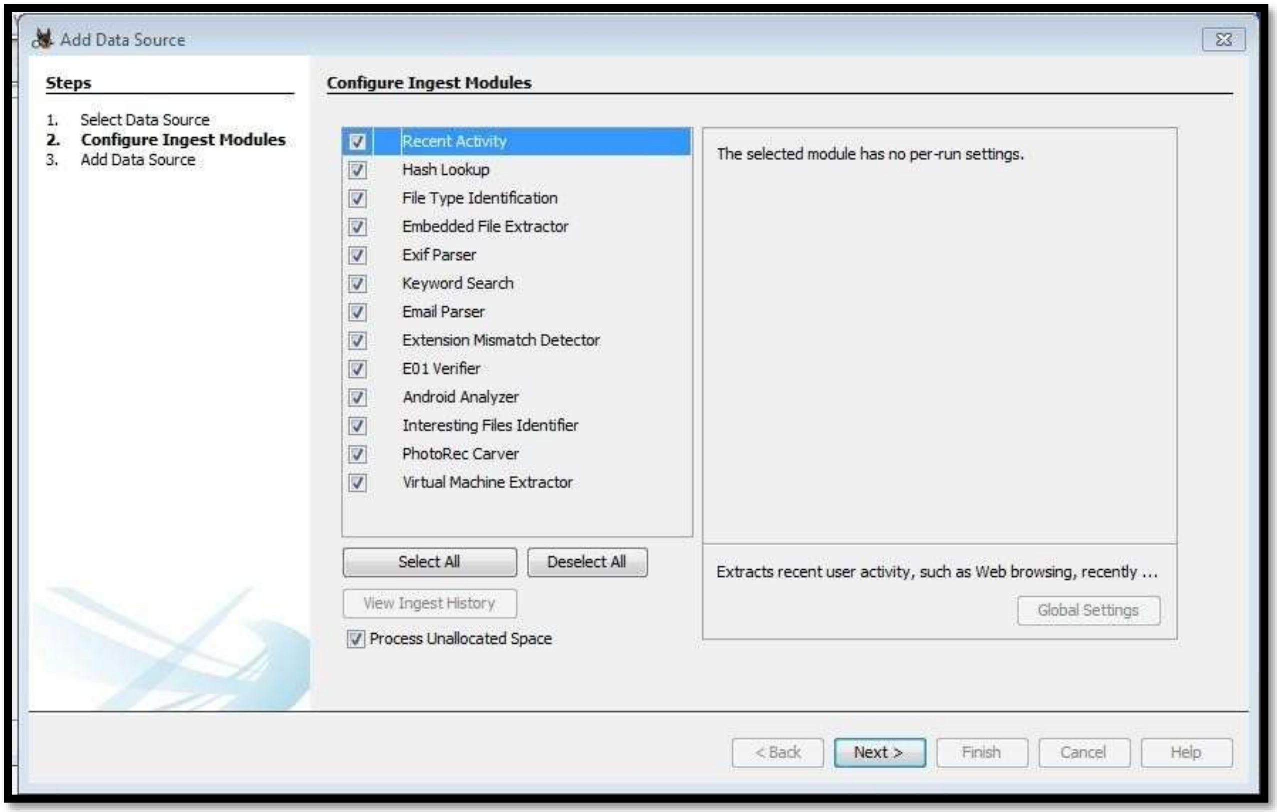
Browse for an image file:

C:\Users\Admin\Desktop\CF TOOLS\WinXp3.iso

Please select the input timezone: (GMT+5:30) Asia/Calcutta

□ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

6. Click Next.



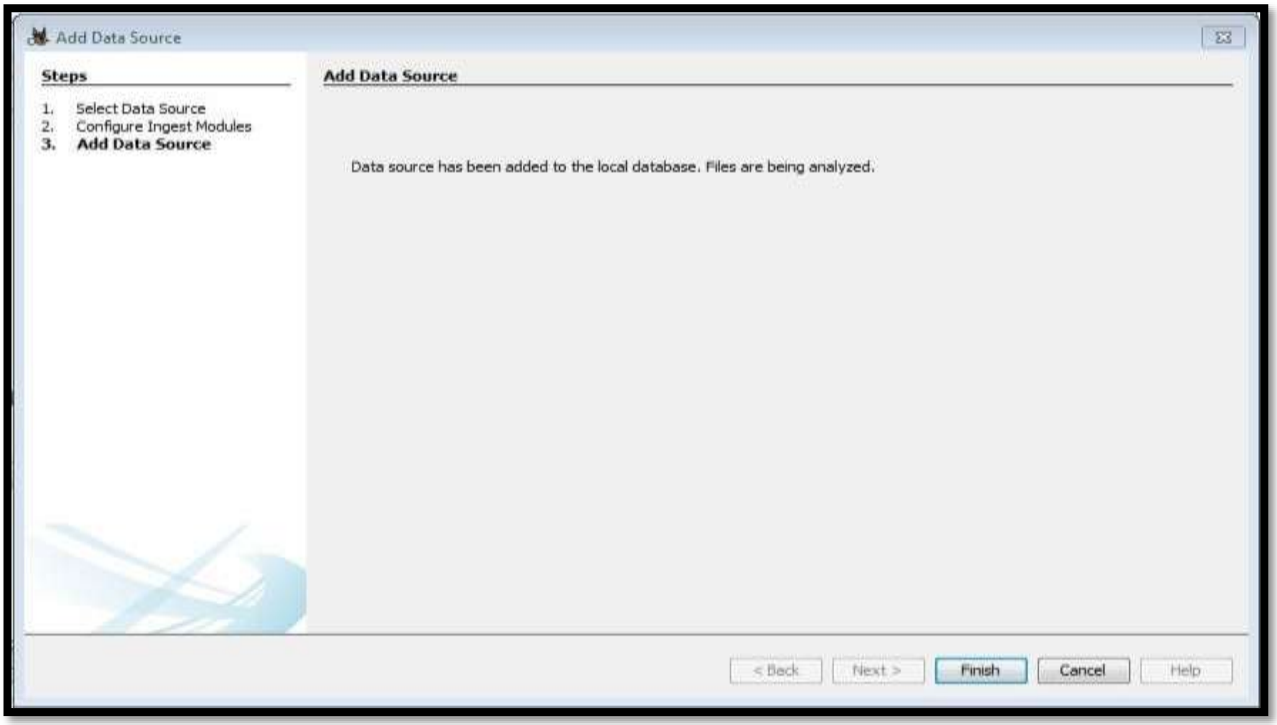
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ Virtual Machine Extractor

☑ Process Unallocated Space

The selected module has no per-run settings.

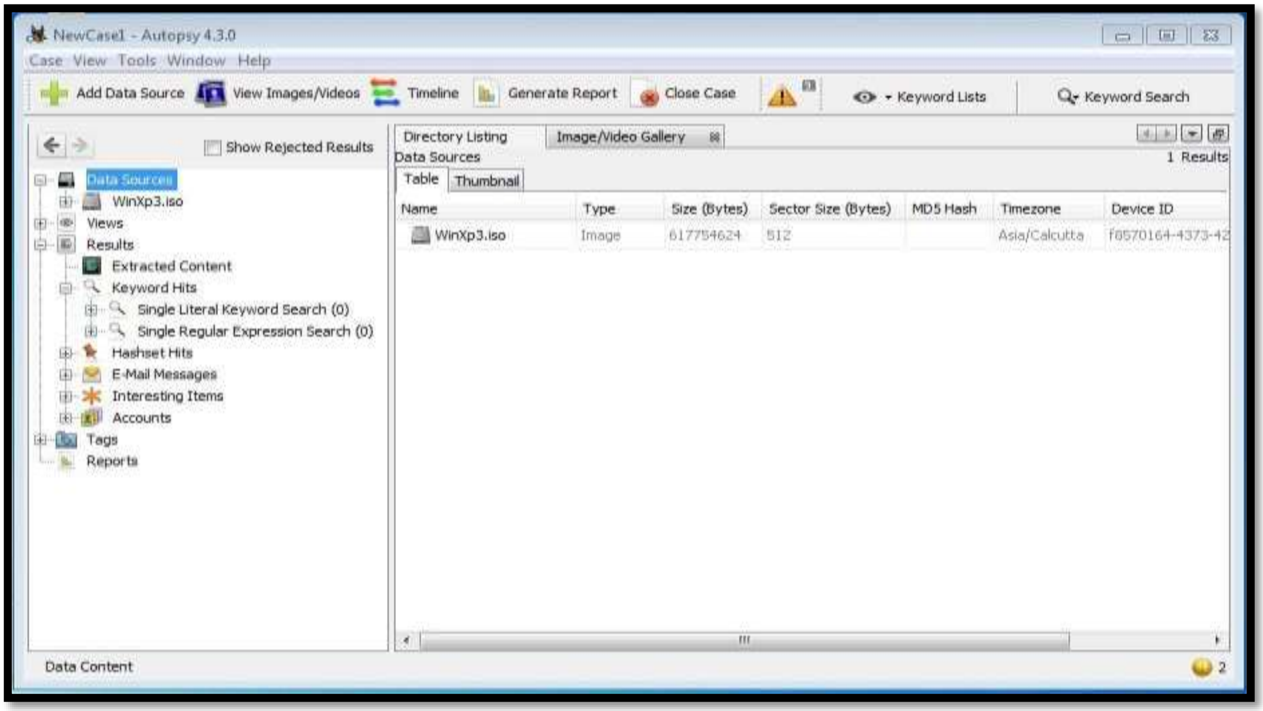
Extracts recent user activity, such as Web browsing, recently ...

7. Data Source will be added. Click Finish.



Data source has been added to the local database. Files are being analyzed.

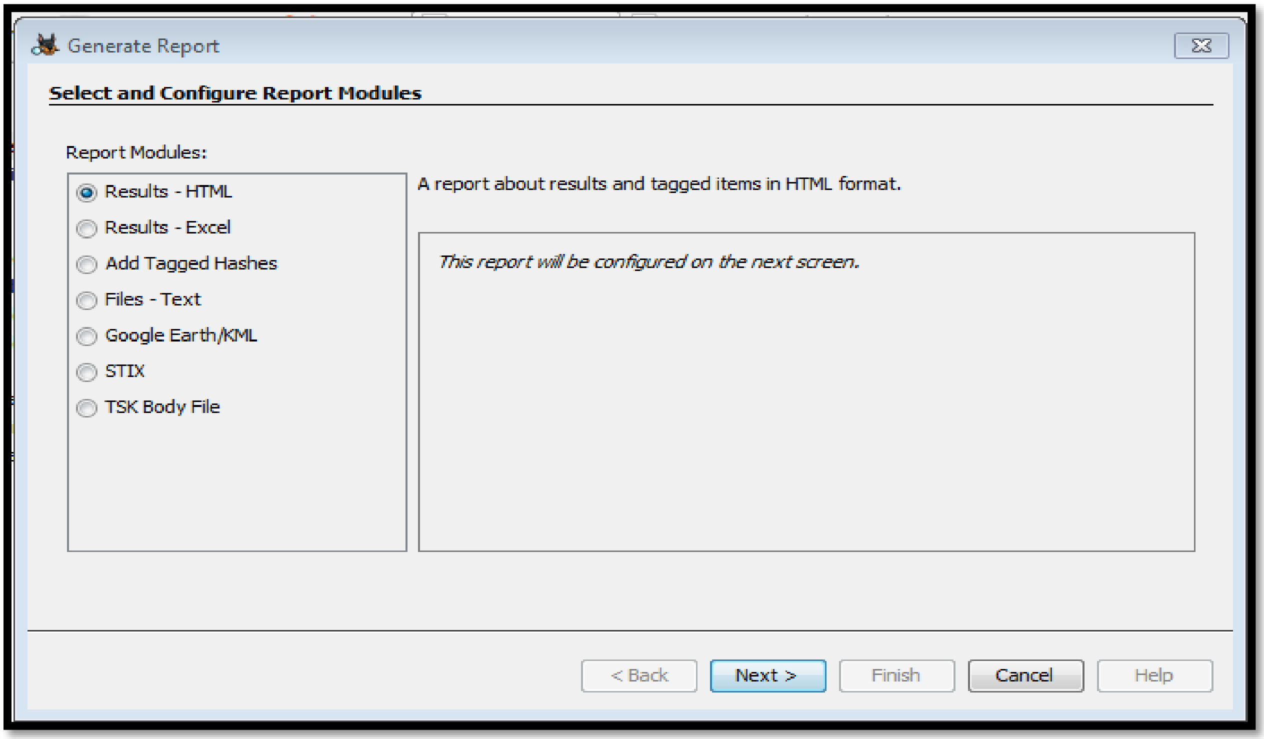
8. You can see the data source added in our case.



Data Sources — 1 Results

Name	Type	Size (Bytes)	Sector Size (Bytes)	MD5 Hash	Timezone	Device ID
WinXp3.iso	Image	617754624	512		Asia/Calcutta	f6570164-4373-42

9. To generate reports, Click on Generate Report & select Report module. We selected HTML.



Select and Configure Report Modules

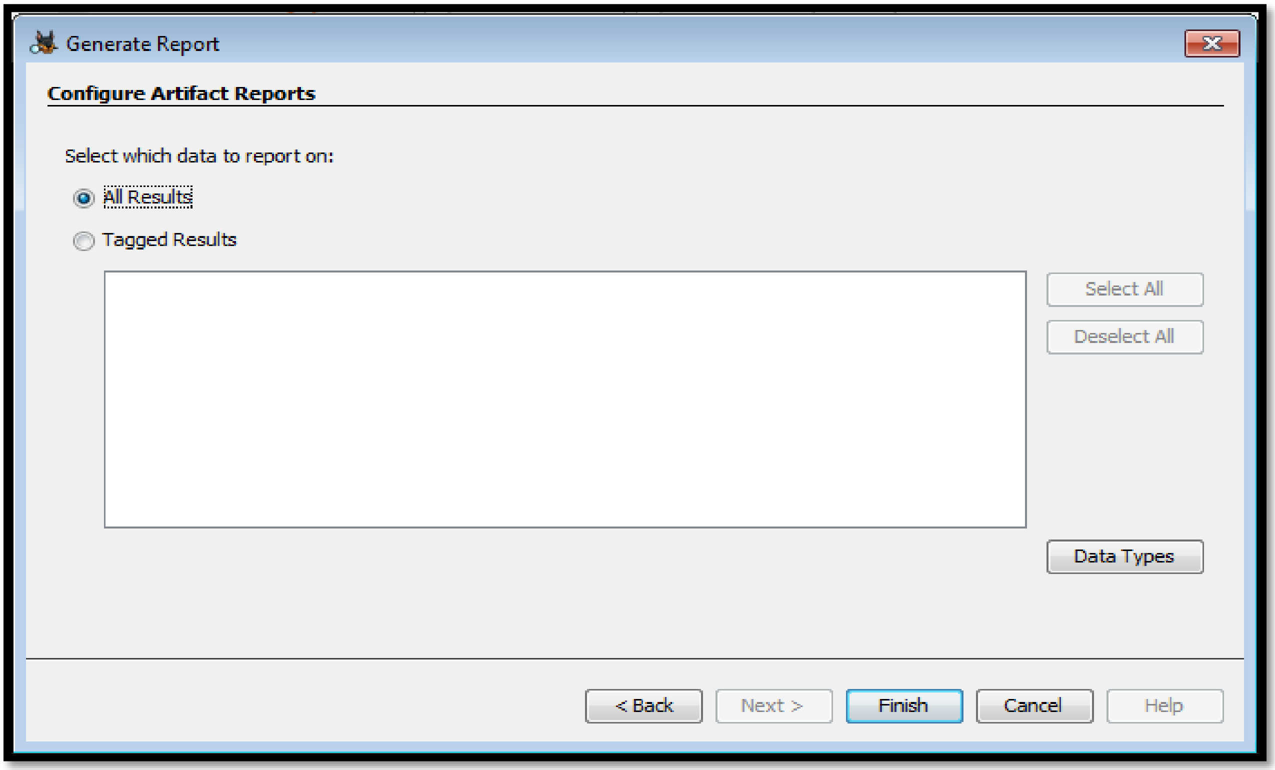
Report Modules:

- ● Results - HTML
- ○ Results - Excel
- ○ Add Tagged Hashes
- ○ Files - Text
- ○ Google Earth/KML
- ○ STIX
- ○ TSK Body File

A report about results and tagged items in HTML format.

This report will be configured on the next screen.

10. Select which data to report on, We selected All Results.

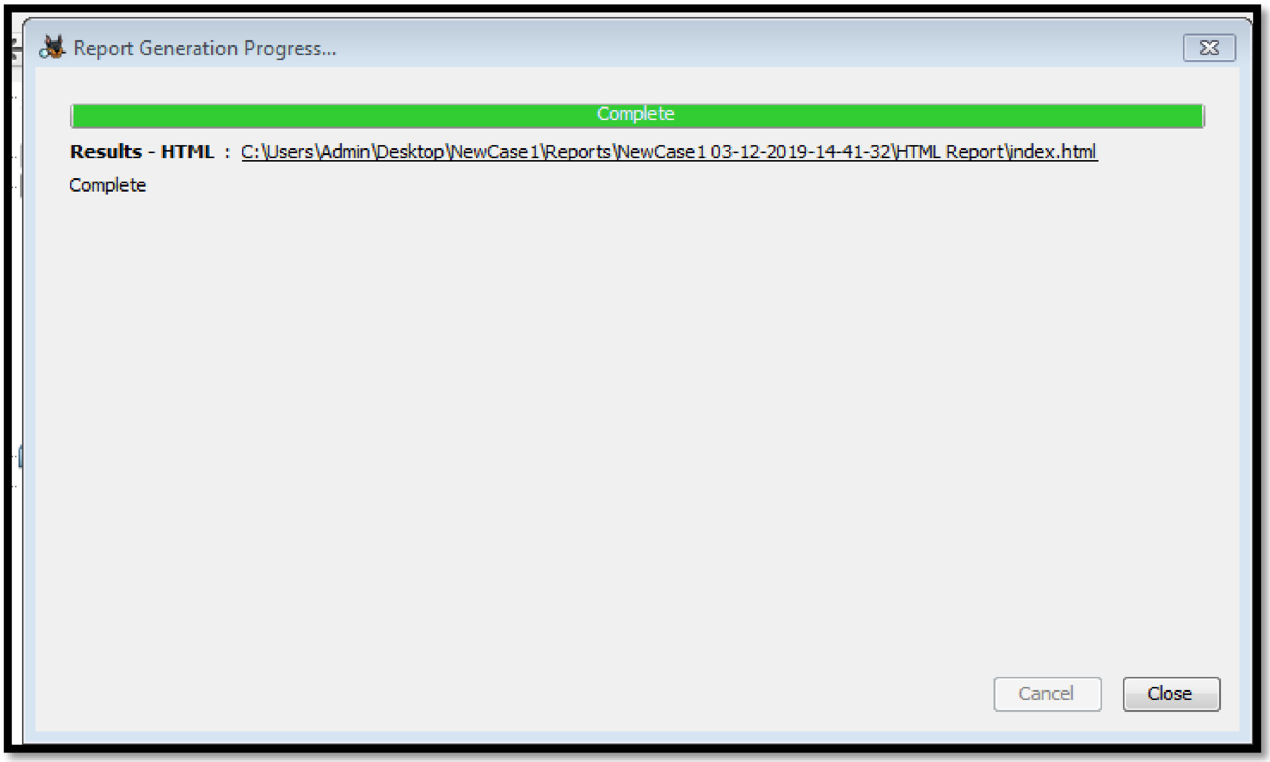


Select which data to report on:

● All Results

○ Tagged Results

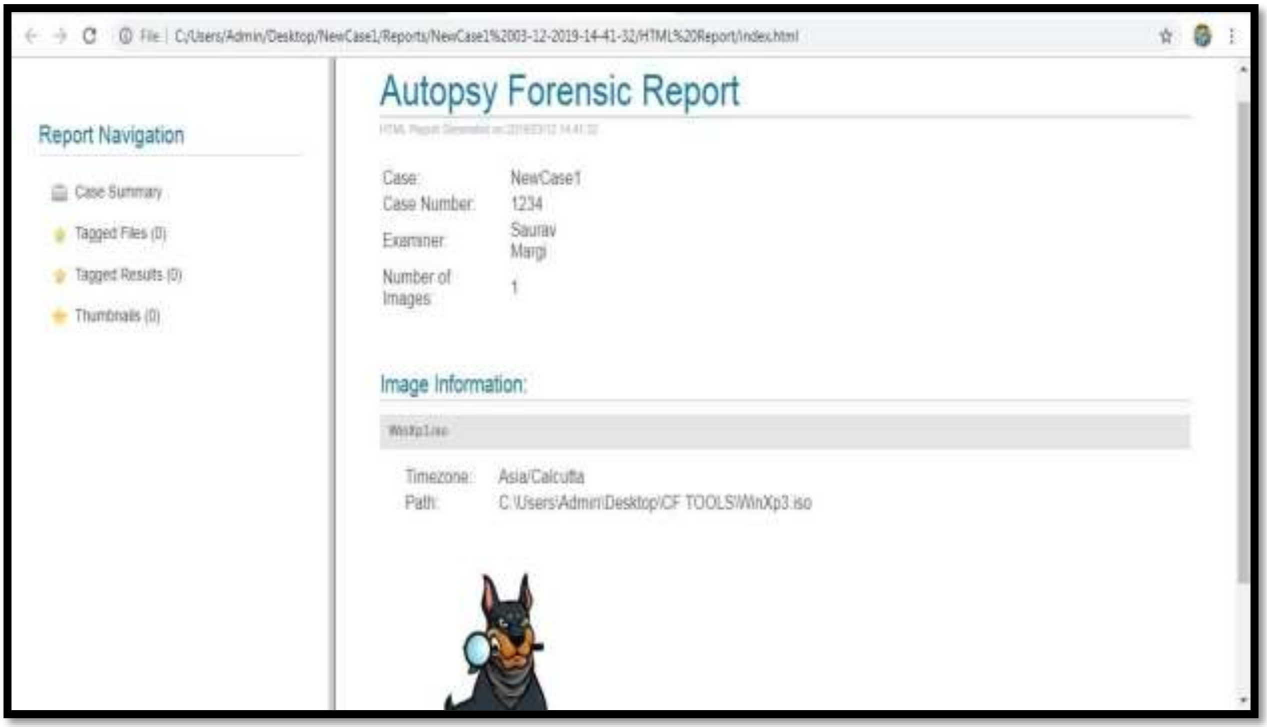
11. Report will be generated.



Results - HTML : C:\Users\Admin\Desktop\NewCase1\Reports\NewCase1 03-12-2019-14-41-32\HTML Report\index.html

Complete

12. The generated report can be displayed as follows:-



File | C:/Users/Admin/Desktop/NewCase1/Reports/NewCase1%2003-12-2019-14-41-32/HTML%20Report/index.html

Report Navigation

- Case Summary
- Tagged Files (0)
- Tagged Results (0)
- Thumbnails (0)

Autopsy Forensic Report

HTML Report Generated on 2019/03/12 14:41:32

Case:	NewCase1
Case Number:	1234
Examiner:	Saurav Margi
Number of Images:	1

Image Information:

WinXp1.iso

Timezone:	Asia/Calcutta
Path:	C:\Users\Admin\Desktop/CF TOOLS\WinXp3.iso

CONCLUSION:- We successfully analyzed the forensic image file using Autopsy

Practical 3

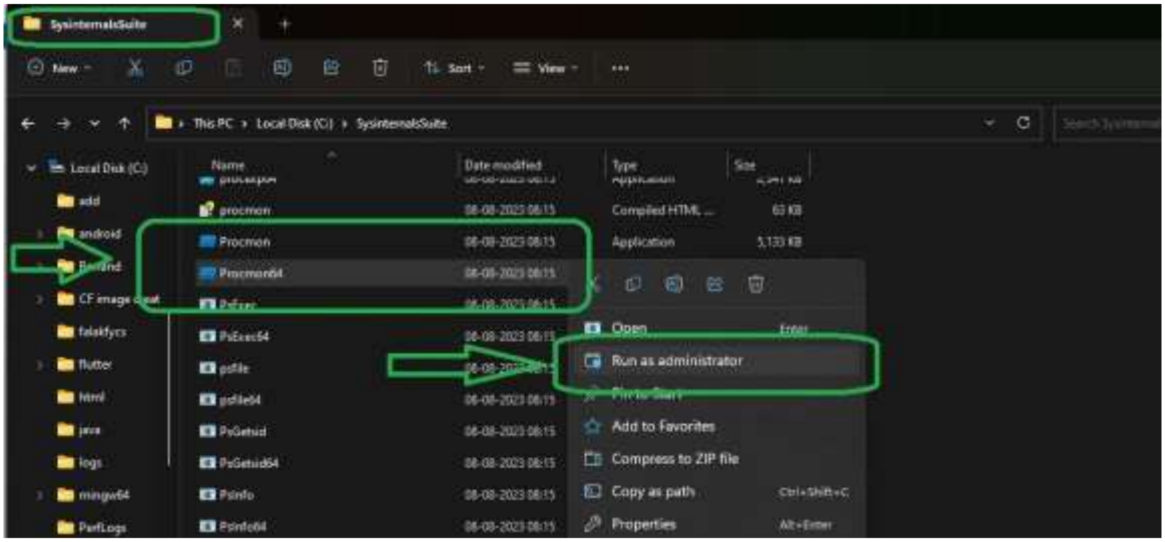
Analyze the memory dump of a running computer system.

- **Extract volatile data, such as open processes, network connections, and registry information.**

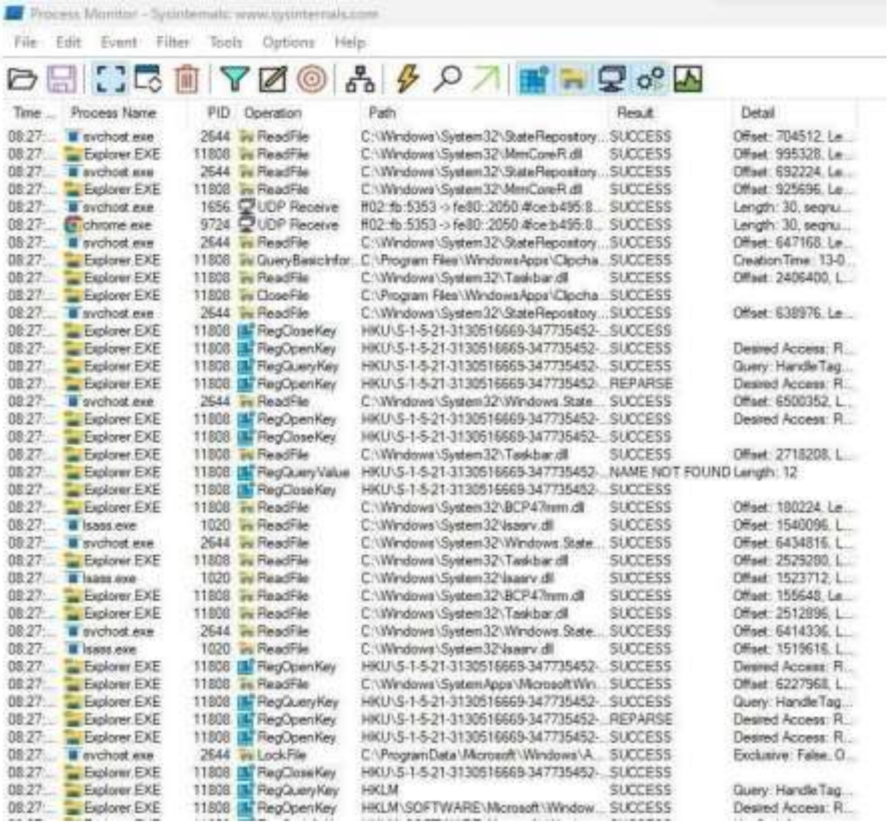
<u>Practical:</u>

<u>Open Process</u>

Go to Sysinternal Suite □ **<u>ProcMon</u>** □Right Click on it and **<u>Open As Administrator</u>**



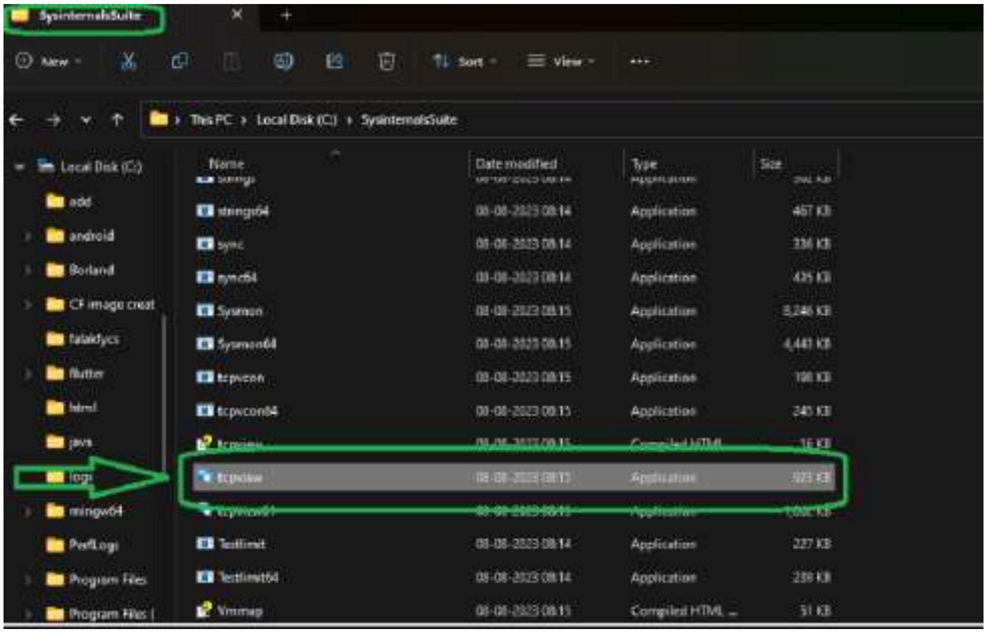
Name	Date modified	Type	Size
procmon	08-08-2023 08:15	Compiled HTML ...	63 KB
Procmon	08-08-2023 08:15	Application	5,133 KB
Procmon64	08-08-2023 08:15		
PsExec	08-08-2023 08:15		
PsExec64	08-08-2023 08:15		
psfile	08-08-2023 08:15		
psfile64	08-08-2023 08:15		
PsGetsid	08-08-2023 08:15		
PsGetsid64	08-08-2023 08:15		
PsInfo	08-08-2023 08:15		
PsInfo64	08-08-2023 08:15		



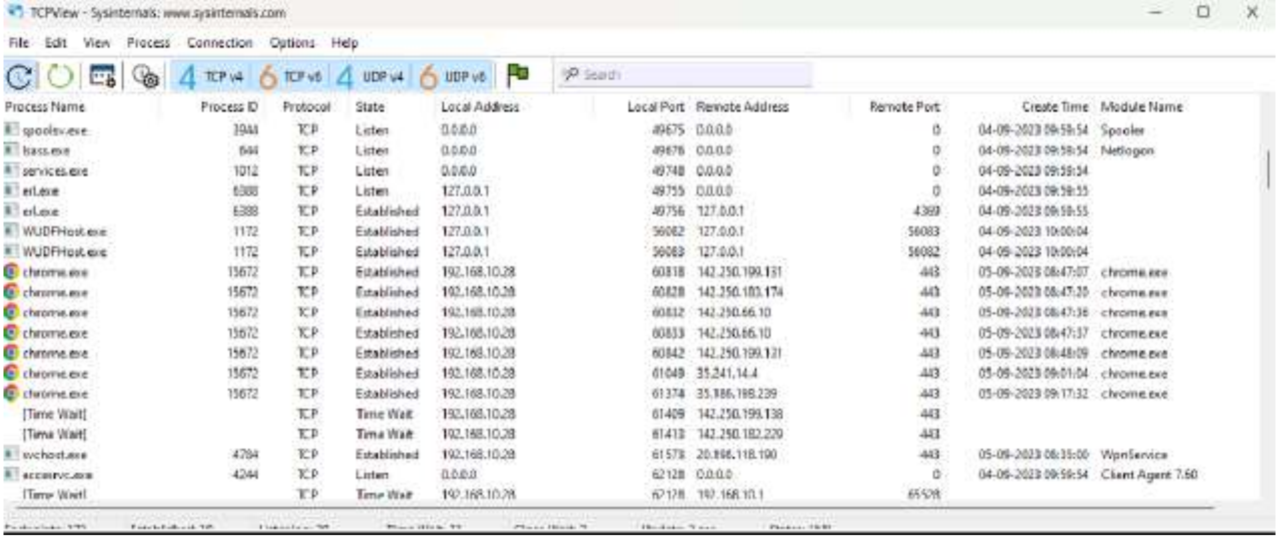
Time ...	Process Name	PID	Operation	Path	Result	Detail
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 704512, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset: 995328, Le...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 692224, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\MrmCoreR.dll	SUCCESS	Offset: 925696, Le...
08:27:...	svchost.exe	1656	UDP Receive	ff02::fb:5353 -> fe80::2050:4ce:b495:8...	SUCCESS	Length: 30, seqnu...
08:27:...	chrome.exe	9724	UDP Receive	ff02::fb:5353 -> fe80::2050:4ce:b495:8...	SUCCESS	Length: 30, seqnu...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 647168, Le...
08:27:...	Explorer.EXE	11808	QueryBasicInfor...	C:\Program Files\WindowsApps\Clipcha...	SUCCESS	CreationTime: 13-0...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2406400, L...
08:27:...	Explorer.EXE	11808	CloseFile	C:\Program Files\WindowsApps\Clipcha...	SUCCESS	
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 638976, Le...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	REPARSE	Desired Access: R...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6500352, L...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2718208, L...
08:27:...	Explorer.EXE	11808	RegQueryValue	HKU\S-1-5-21-3130516669-347735452-...	NAME NOT FOUND	Length: 12
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP47mrm.dll	SUCCESS	Offset: 180224, Le...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1540096, L...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6434816, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2529280, L...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1523712, L...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\BCP47mrm.dll	SUCCESS	Offset: 155648, Le...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2512896, L...
08:27:...	svchost.exe	2644	ReadFile	C:\Windows\System32\Windows.State...	SUCCESS	Offset: 6414336, L...
08:27:...	lsass.exe	1020	ReadFile	C:\Windows\System32\lsasrv.dll	SUCCESS	Offset: 1519616, L...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Desired Access: R...
08:27:...	Explorer.EXE	11808	ReadFile	C:\Windows\SystemApps\MicrosoftWin...	SUCCESS	Offset: 6227968, L...
08:27:...	Explorer.EXE	11808	RegQueryKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	REPARSE	Desired Access: R...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	Desired Access: R...
08:27:...	svchost.exe	2644	LockFile	C:\ProgramData\Microsoft\Windows\A...	SUCCESS	Exclusive: False, O...
08:27:...	Explorer.EXE	11808	RegCloseKey	HKU\S-1-5-21-3130516669-347735452-...	SUCCESS	
08:27:...	Explorer.EXE	11808	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
08:27:...	Explorer.EXE	11808	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...

- ## Network Connections

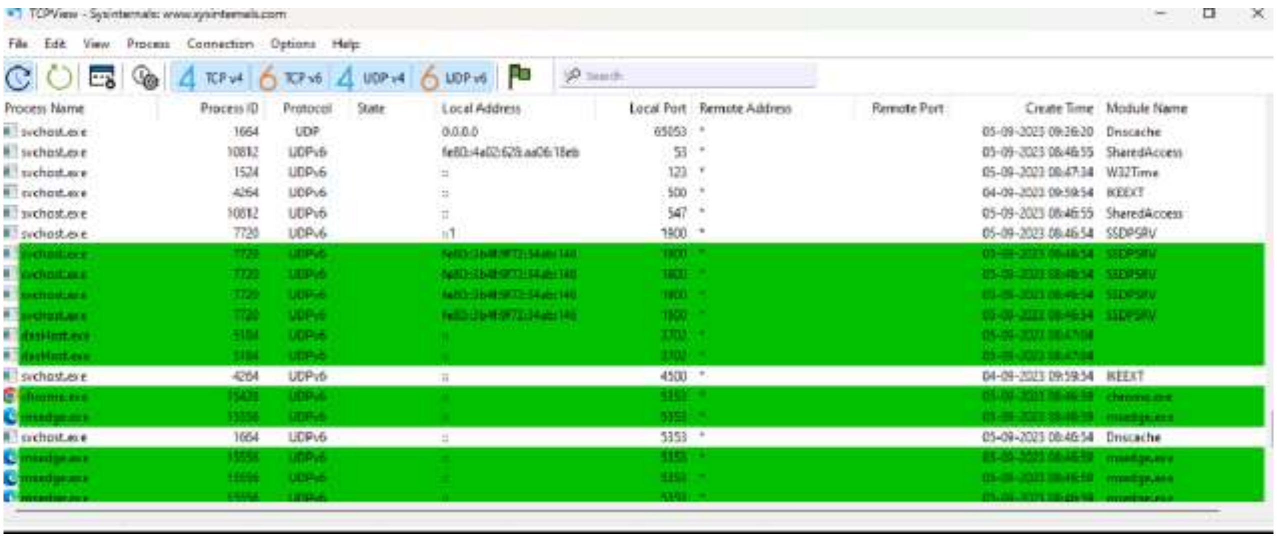
Go to SysinternalSuite TCPview



Name	Date modified	Type	Size
strings64	08-08-2023 08:14	Application	467 KB
sync	08-08-2023 08:14	Application	336 KB
sync64	08-08-2023 08:14	Application	435 KB
Sysmon	08-08-2023 08:15	Application	8,246 KB
Sysmon64	08-08-2023 08:15	Application	4,440 KB
tcpvcon	08-08-2023 08:15	Application	198 KB
tcpvcon64	08-08-2023 08:15	Application	240 KB
tcpview	08-08-2023 08:15	Compiled HTML	16 KB
tcpview	08-08-2023 08:15	Application	923 KB
tcpview64	08-08-2023 08:15	Application	[illegible]
Testlimit	08-08-2023 08:14	Application	227 KB
Testlimit64	08-08-2023 08:14	Application	239 KB
Vmmap	08-08-2023 08:15	Compiled HTML ...	51 KB


TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
4 TCP v4
6 TCP v6
4 UDP v4
6 UDP v6
Search

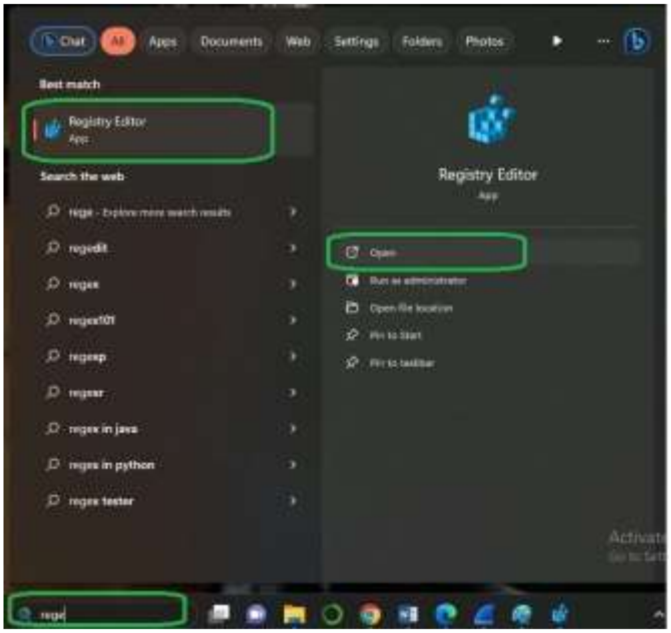
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
spoolsv.exe	3944	TCP	Listen	0.0.0.0	49675	0.0.0.0	0	04-09-2023 09:59:54	Spooler
lsass.exe	844	TCP	Listen	0.0.0.0	49676	0.0.0.0	0	04-09-2023 09:59:54	Netlogon
services.exe	1012	TCP	Listen	0.0.0.0	49748	0.0.0.0	0	04-09-2023 09:59:54	
erl.exe	6388	TCP	Listen	127.0.0.1	49755	0.0.0.0	0	04-09-2023 09:59:55	
erl.exe	6388	TCP	Established	127.0.0.1	49756	127.0.0.1	4369	04-09-2023 09:59:55	
WUDFHost.exe	1172	TCP	Established	127.0.0.1	56082	127.0.0.1	56083	04-09-2023 10:00:04	
WUDFHost.exe	1172	TCP	Established	127.0.0.1	56083	127.0.0.1	56082	04-09-2023 10:00:04	
chrome.exe	15672	TCP	Established	192.168.10.28	60818	142.250.199.131	443	05-09-2023 08:47:07	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60828	142.250.183.174	443	05-09-2023 08:47:20	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60832	142.250.66.10	443	05-09-2023 08:47:36	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60833	142.250.66.10	443	05-09-2023 08:47:37	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	60842	142.250.199.131	443	05-09-2023 08:48:09	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	61049	35.241.14.4	443	05-09-2023 09:01:04	chrome.exe
chrome.exe	15672	TCP	Established	192.168.10.28	61374	35.186.198.239	443	05-09-2023 09:17:32	chrome.exe
[Time Wait]		TCP	Time Wait	192.168.10.28	61409	142.250.199.138	443		
[Time Wait]		TCP	Time Wait	192.168.10.28	61413	142.250.182.220	443		
svchost.exe	4784	TCP	Established	192.168.10.28	61578	20.198.118.190	443	05-09-2023 08:35:00	WpnService
accsvc.exe	4244	TCP	Listen	0.0.0.0	62128	0.0.0.0	0	04-09-2023 09:59:54	Client Agent 7.60
[Time Wait]		TCP	Time Wait	192.168.10.28	62178	192.168.10.1	65528		


TCPView - Sysinternals: www.sysinternals.com
File Edit View Process Connection Options Help
4 TCP v4
6 TCP v6
4 UDP v4
6 UDP v6
Search

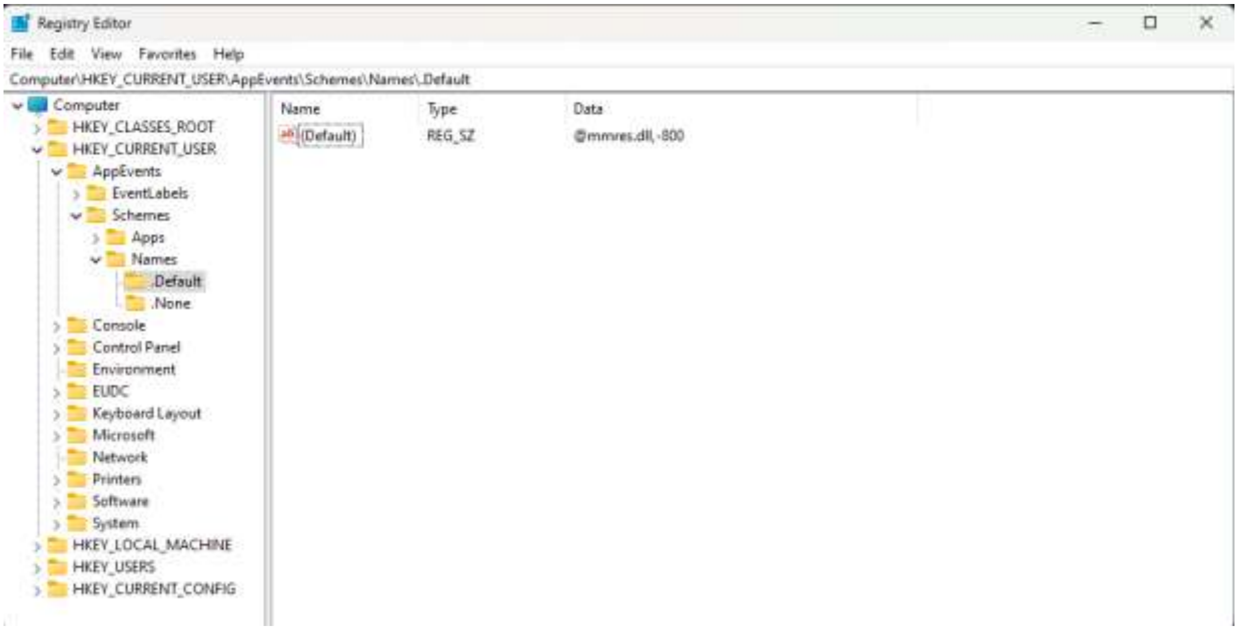
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1664	UDP		0.0.0.0	65053	*		05-09-2023 09:26:20	Dnscache
svchost.exe	10812	UDPv6		fe80::4e02:628:aa06:18eb	53	*		05-09-2023 08:46:55	SharedAccess
svchost.exe	1524	UDPv6		::	123	*		05-09-2023 08:47:34	W32Time
svchost.exe	4264	UDPv6		::	500	*		04-09-2023 09:59:54	IKEEXT
svchost.exe	10812	UDPv6		::	547	*		05-09-2023 08:46:55	SharedAccess
svchost.exe	7720	UDPv6		::1	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b48:9f72:34ab:140	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b48:9f72:34ab:140	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b48:9f72:34ab:140	1900	*		05-09-2023 08:46:54	SSDPSRV
svchost.exe	7720	UDPv6		fe80::3b48:9f72:34ab:140	1900	*		05-09-2023 08:46:54	SSDPSRV
dasHost.exe	5184	UDPv6		::	3702	*		05-09-2023 08:47:04	
dasHost.exe	5184	UDPv6		::	3702	*		05-09-2023 08:47:04	
svchost.exe	4264	UDPv6		::	4500	*		04-09-2023 09:59:54	IKEEXT
chrome.exe	15420	UDPv6		::	5353	*		05-09-2023 08:46:59	chrome.exe
msedge.exe	13356	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
svchost.exe	1664	UDPv6		::	5353	*		05-09-2023 08:46:54	Dnscache
msedge.exe	13356	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
msedge.exe	13356	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe
msedge.exe	13356	UDPv6		::	5353	*		05-09-2023 08:46:59	msedge.exe

Registry Information

Click on **Search Bar** on the **Taskbar** □ Type **Regedit** □ Click on **Registry Editor**



View the desired registries to be analyzed



Computer\HKEY_CURRENT_USER\AppEvents\Schemes\Names\.Default

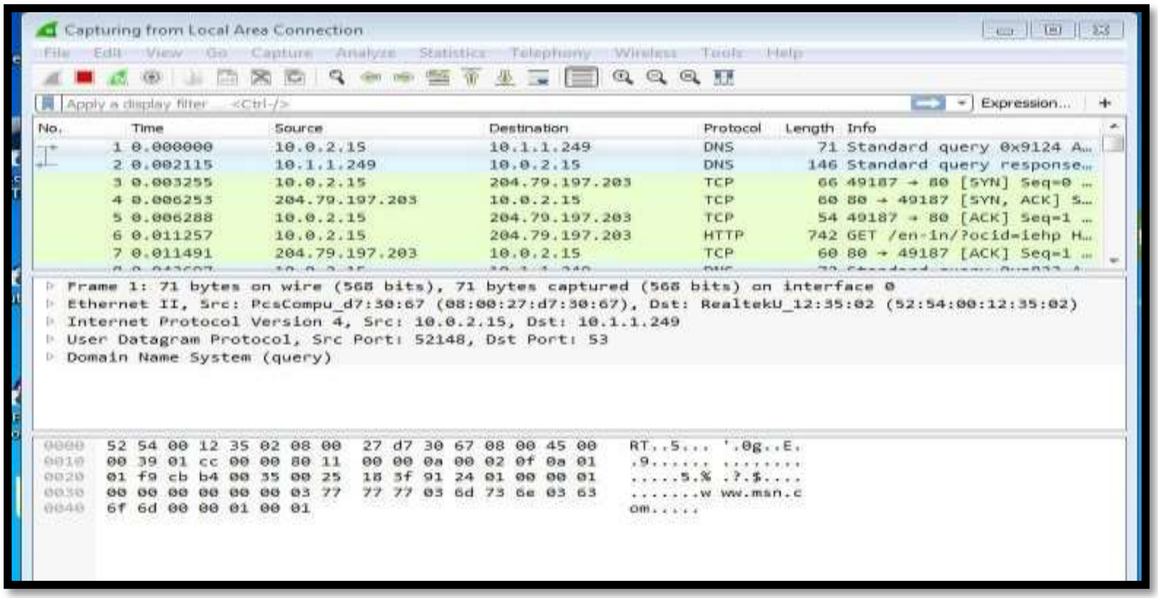
Name	Type	Data
(Default)	REG_SZ	@mmres.dll,-800

Practical 4

Aim :- Capturing and analyzing network packets using Wireshark (Fundamentals) : -
-Identification the live network
-Capture Packets
-Analyze the captured packets

Step 1:-

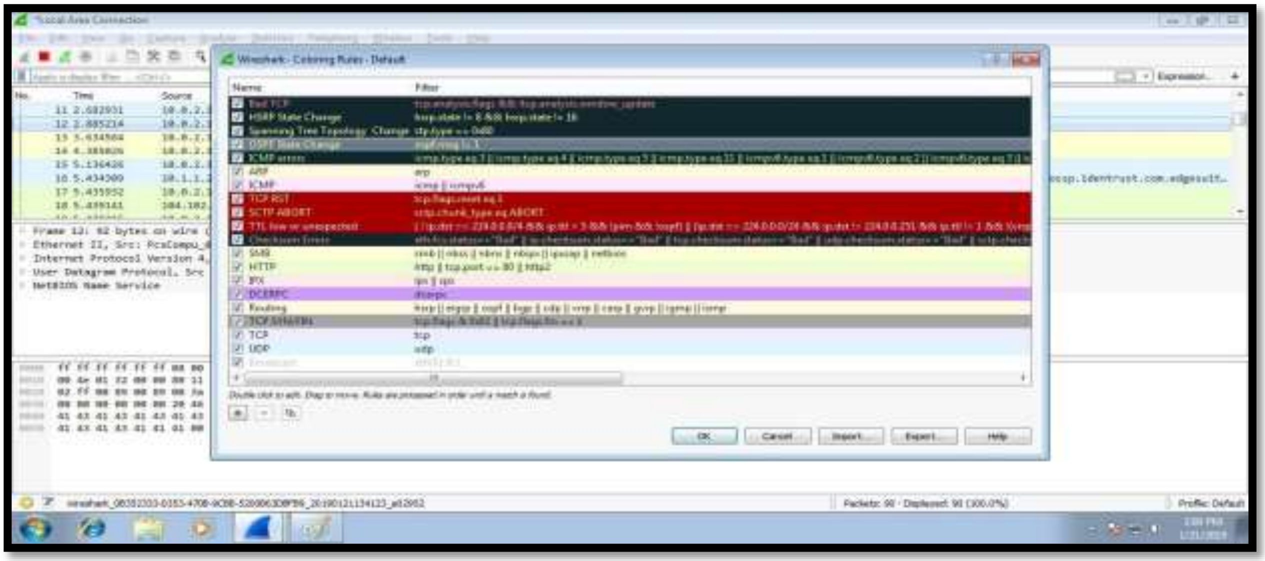
Start Wireshark and Double click on Local Area Connections.



Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.     Time        Source          Destination     Protocol  Length Info
      1 0.000000    10.0.2.15       10.1.1.249      DNS           71 Standard query 0x9124 A…
      2 0.002115    10.1.1.249      10.0.2.15       DNS          146 Standard query response…
      3 0.003255    10.0.2.15       204.79.197.203  TCP           66 49187 → 80 [SYN] Seq=0 …
      4 0.006253    204.79.197.203  10.0.2.15       TCP           60 80 → 49187 [SYN, ACK] S…
      5 0.006288    10.0.2.15       204.79.197.203  TCP           54 49187 → 80 [ACK] Seq=1 …
      6 0.011257    10.0.2.15       204.79.197.203  HTTP         742 GET /en-in/?ocid=iehp H…
      7 0.011491    204.79.197.203  10.0.2.15       TCP           60 80 → 49187 [ACK] Seq=1 …

▷ Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▷ Ethernet II, Src: PcsCompu_d7:30:67 (08:00:27:d7:30:67), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▷ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.1.1.249
▷ User Datagram Protocol, Src Port: 52148, Dst Port: 53
▷ Domain Name System (query)

0000  52 54 00 12 35 02 08 00  27 d7 30 67 08 00 45 00   RT..5... '.0g..E.
0010  00 39 01 cc 00 00 80 11  00 00 0a 00 02 0f 0a 01   .9...... ........
0020  01 f9 cb b4 00 35 00 25  18 3f 91 24 01 00 00 01   .....5.% .?.$....
0030  00 00 00 00 00 00 03 77  77 77 03 6d 73 6e 03 63   .......w ww.msn.c
0040  6f 6d 00 00 01 00 01                               om.....
```

Step 2:-
To Know the Meanings of Colours Go to View Colouring Rules



Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 [illegible]
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && [illegible]
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.check[illegible]
☑ SMB	smb || nbss || nbns || nbipx || ipxsap || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ IPX	ipx || spx
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1

Double click to edit. Drag to move. Rules are processed in order until a match is found.

wireshark_[illegible]_20190121134123_a02962

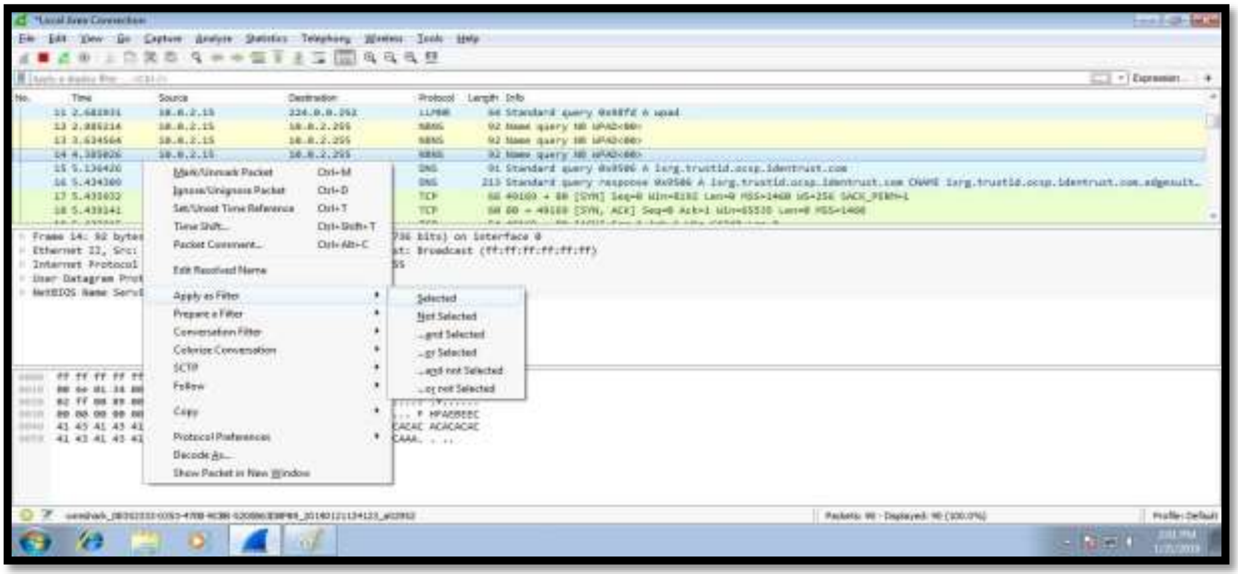
Packets: 90 · Displayed: 90 (100.0%)

Profile: Default

Step 3:-

To Analyse captured packet

Select any Process Apply as filter Selected



```
No.   Time        Source       Destination   Protocol Length Info
   11 2.682031    10.0.2.15    224.0.0.252   LLMNR      64 Standard query 0x88fd A wpad
   12 2.885214    10.0.2.15    10.0.2.255    NBNS       92 Name query NB WPAD<00>
   13 3.634564    10.0.2.15    10.0.2.255    NBNS       92 Name query NB WPAD<00>
   14 4.385026    10.0.2.15    10.0.2.255    NBNS       92 Name query NB WPAD<00>
   15 5.136420                              DNS        81 Standard query 0x9506 A lsrg.trustid.ocsp.identrust.com
   16 5.434300                              DNS       213 Standard query response 0x9506 A lsrg.trustid.ocsp.identrust.com CNAME lsrg.trustid.ocsp.identrust.com.edgesuit...
   17 5.433032                              TCP        66 49169 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
   18 5.433141                              TCP        60 80 → 49169 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
```

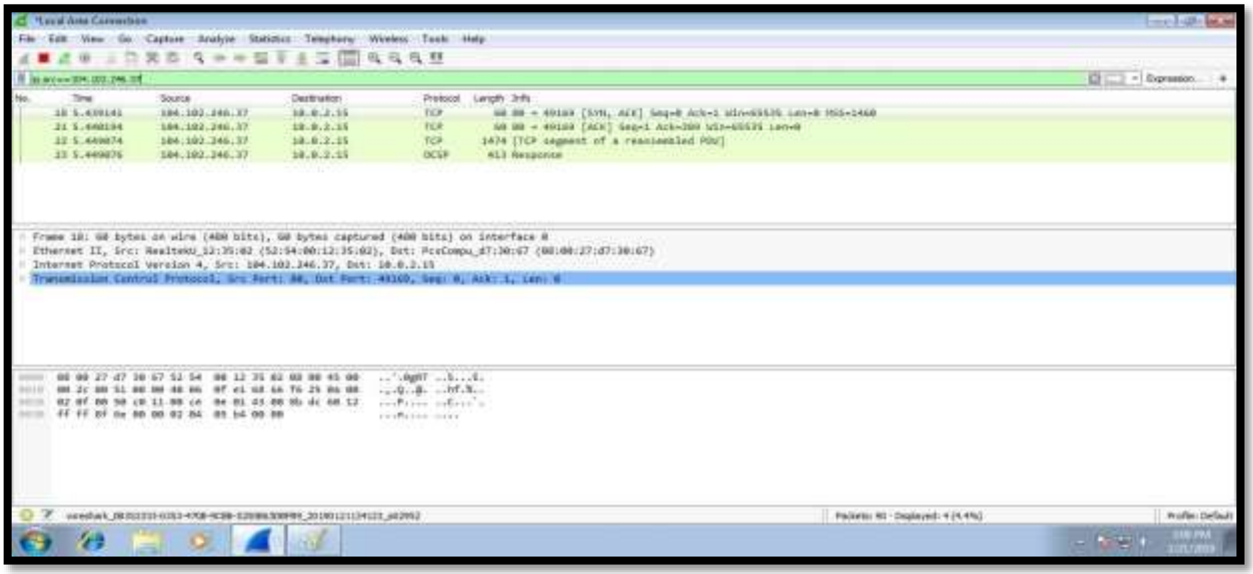
```
Frame 14: 92 bytes ... (736 bits) on interface 0
Ethernet II, Src: ... Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol ...
User Datagram Prot...
NetBIOS Name Servi...
```

Step 4:- Now here are some filter commands:-

- Source Packets :-

  It displays packets coming from specific IP Address.

  Eg :- ip.src ==104.102.246.37


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

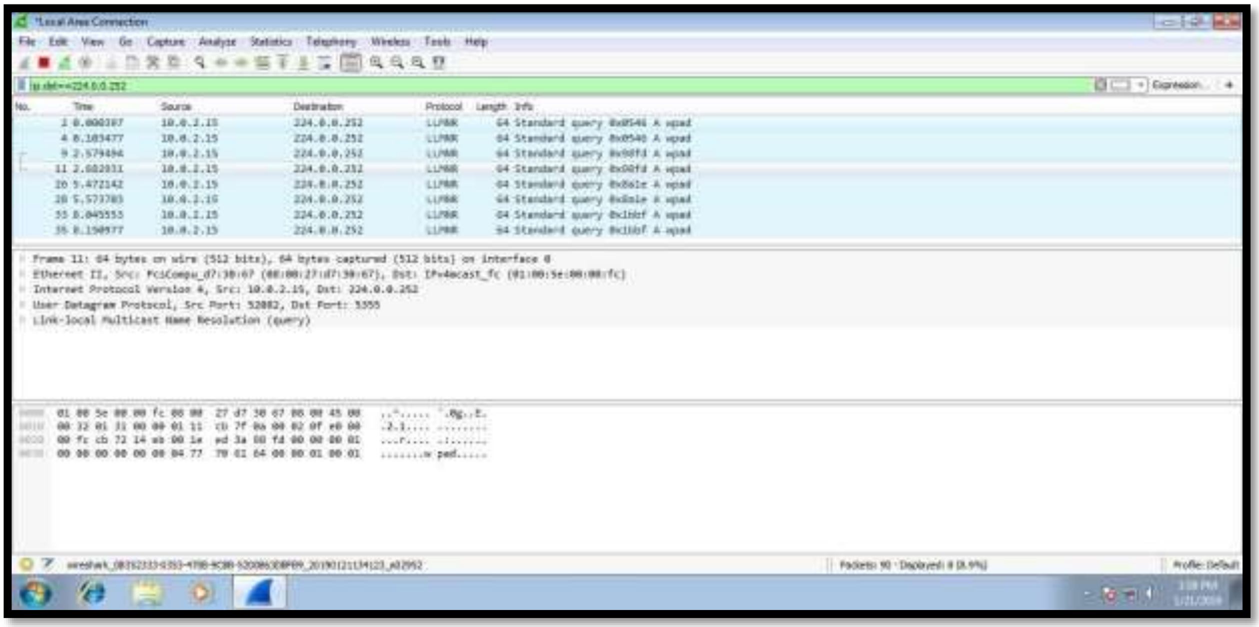
```
ip.src==104.102.246.37
```

```
No.   Time        Source           Destination   Protocol Length Info
   18 5.439141    104.102.246.37   10.0.2.15     TCP        60 80 → 49169 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   21 5.440194    104.102.246.37   10.0.2.15     TCP        60 80 → 49169 [ACK] Seq=1 Ack=300 Win=65535 Len=0
   22 5.449874    104.102.246.37   10.0.2.15     TCP      1474 [TCP segment of a reassembled PDU]
   23 5.449876    104.102.246.37   10.0.2.15     OCSP      413 Response
```

```
Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d7:30:67 (08:00:27:d7:30:67)
Internet Protocol Version 4, Src: 104.102.246.37, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 49169, Seq: 0, Ack: 1, Len: 0
```

- Destination Packets :-
  It displays packets having specific IP Address as Destination.

  Eg :- ip.dst ==225.0.0.252



*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst==224.0.0.252
Expression...

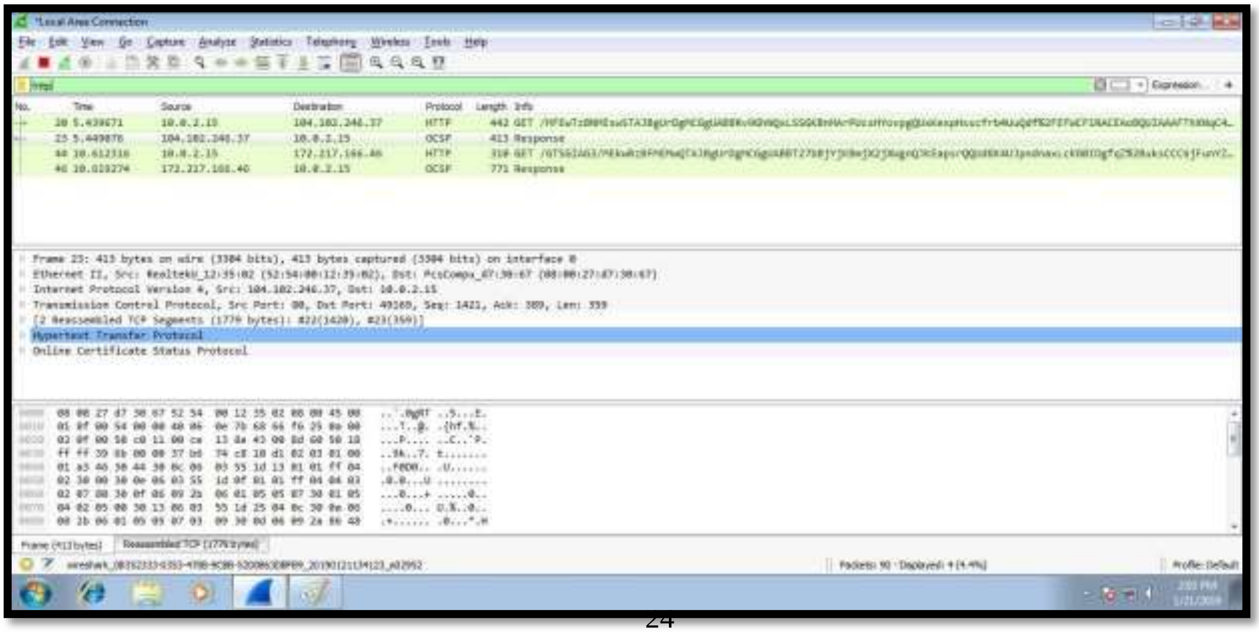
```
No.    Time         Source       Destination   Protocol  Length  Info
     2 0.000387     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x0546 A wpad
     4 0.103477     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x0546 A wpad
     9 2.579494     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x98fd A wpad
    11 2.682031     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x98fd A wpad
    26 5.472142     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x861e A wpad
    28 5.573703     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x861e A wpad
    35 8.045553     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x1bbf A wpad
    36 8.150977     10.0.2.15    224.0.0.252   LLMNR         64  Standard query 0x1bbf A wpad

Frame 11: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
Ethernet II, Src: PcsCompu_d7:30:67 (08:00:27:d7:30:67), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 224.0.0.252
User Datagram Protocol, Src Port: 52082, Dst Port: 5355
Link-local Multicast Name Resolution (query)

0000  01 00 5e 00 00 fc 08 00  27 d7 30 67 08 00 45 00   ..^..... '.0g..E.
0010  00 32 01 31 00 00 01 11  cb 7f 0a 00 02 0f e0 00   .2.1.... ........
0020  00 fc cb 72 14 eb 00 1e  ed 3a 00 fd 00 00 00 01   ...r.... .:......
0030  00 00 00 00 00 00 04 77  70 61 64 00 00 01 00 01   .......w pad.....
```

wireshark_[illegible]_20190121134123_a02952
Packets: 90 · Displayed: 8 (8.9%)
Profile: Default

- http Packets :-

  It displays packets which are having http protocol.

  Eg :- http

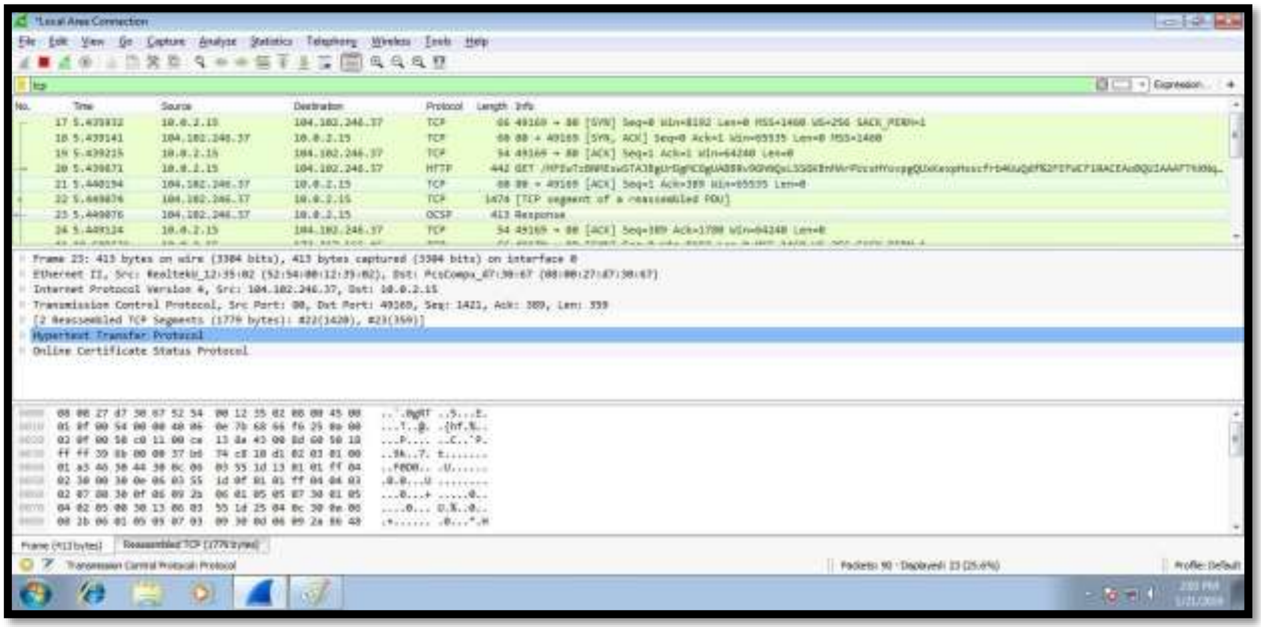


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.    Time         Source           Destination      Protocol  Length  Info
    20 5.439671     10.0.2.15        104.102.246.37   HTTP         442  GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABB[illegible]
    23 5.449876     104.102.246.37   10.0.2.15        OCSP         413  Response
    44 10.612316    10.0.2.15        172.217.166.46   HTTP         310  GET /GTSGIAG3/[illegible]
    46 10.020274    172.217.166.46   10.0.2.15        OCSP         771  Response

Frame 23: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d7:30:67 (08:00:27:d7:30:67)
Internet Protocol Version 4, Src: 104.102.246.37, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 49169, Seq: 1421, Ack: 389, Len: 359
[2 Reassembled TCP Segments (1779 bytes): #22(1420), #23(359)]
Hypertext Transfer Protocol
Online Certificate Status Protocol

0000  08 00 27 d7 30 67 52 54  00 12 35 02 08 00 45 00   ..'.0gRT ..5...E.
0010  01 8f 00 54 00 00 40 06  0e 7b 68 66 f6 25 0a 00   ...T..@. .{hf.%..
0020  02 0f 00 50 c0 11 00 ca  13 da 43 00 8d 60 50 18   ...P.... ..C..`P.
0030  ff ff 39 8b 00 00 37 b6  74 c8 18 d1 82 03 01 00   ..9k..7. t.......
0040  01 a3 40 30 44 30 8c 06  09 55 1d 13 01 01 ff 04   ..F0D0.. .U......
0050  02 30 00 30 0e 06 03 55  1d 0f 01 01 ff 04 04 03   .0.0...U ........
0060  02 07 80 30 0f 06 09 2b  06 01 05 05 07 30 01 05   ...0...+ .....0..
0070  04 02 05 00 30 13 06 03  55 1d 25 04 0c 30 0a 06   ....0... U.%..0..
0080  08 2b 06 01 05 05 07 03  09 30 0d 06 09 2a 86 48   .+...... .0...*.H
```

Frame (413 bytes)
Reassembled TCP (1779 bytes)
wireshark_[illegible]_20190121134123_a02952
Packets: 90 · Displayed: 4 (4.4%)
Profile: Default

- TCP Packets:-It displays packets having TCP protocol.



*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

```
tcp
```

```
No.  Time        Source          Destination     Protocol Length Info
  17 5.439332    10.0.2.15       104.102.246.37  TCP        66 49169 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  18 5.439141    104.102.246.37  10.0.2.15       TCP        60 80 → 49169 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  19 5.439215    10.0.2.15       104.102.246.37  TCP        54 49169 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  20 5.439871    10.0.2.15       104.102.246.37  HTTP      442 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRv9GVWQsL3S0KBnhWrPzcsHYozpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAs0QUIAAAFTkX0q…
  21 5.440194    104.102.246.37  10.0.2.15       TCP        60 80 → 49169 [ACK] Seq=1 Ack=389 Win=65535 Len=0
  22 5.449876    104.102.246.37  10.0.2.15       TCP      1474 [TCP segment of a reassembled PDU]
  23 5.449876    104.102.246.37  10.0.2.15       OCSP      413 Response
  24 5.449124    10.0.2.15       104.102.246.37  TCP        54 49169 → 80 [ACK] Seq=389 Ack=1780 Win=64240 Len=0
```

```
Frame 23: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d7:30:67 (08:00:27:d7:30:67)
Internet Protocol Version 4, Src: 104.102.246.37, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 49169, Seq: 1421, Ack: 389, Len: 359
[2 Reassembled TCP Segments (1779 bytes): #22(1420), #23(359)]
Hypertext Transfer Protocol
Online Certificate Status Protocol
```

```
0000  08 00 27 d7 30 67 52 54  00 12 35 02 08 00 45 00   ..'.0gRT ..5...E.
0010  01 8f 00 54 00 00 40 06  0e 7b 68 66 f6 25 0a 00   ...T..@. .{hf.%..
0020  02 0f 00 50 c0 11 00 ca  13 da 43 00 8d 60 50 18   ...P.... ..C..`P.
0030  ff ff 39 8b 00 00 37 b6  74 c8 10 d1 02 03 01 00   ..9k..7. t.......
0040  01 a3 46 30 44 30 0c 06  03 55 1d 13 01 01 ff 04   ..F0D0.. .U......
0050  02 30 00 30 0e 06 03 55  1d 0f 01 01 ff 04 04 03   .0.0...U ........
0060  02 07 80 30 0f 06 09 2b  06 01 05 05 07 30 01 05   ...0...+ .....0..
0070  04 02 05 00 30 13 06 03  55 1d 25 04 0c 30 0a 06   ....0... U.%..0..
0080  08 2b 06 01 05 05 07 03  09 30 0d 06 09 2a 86 48   .+...... .0...*.H
```

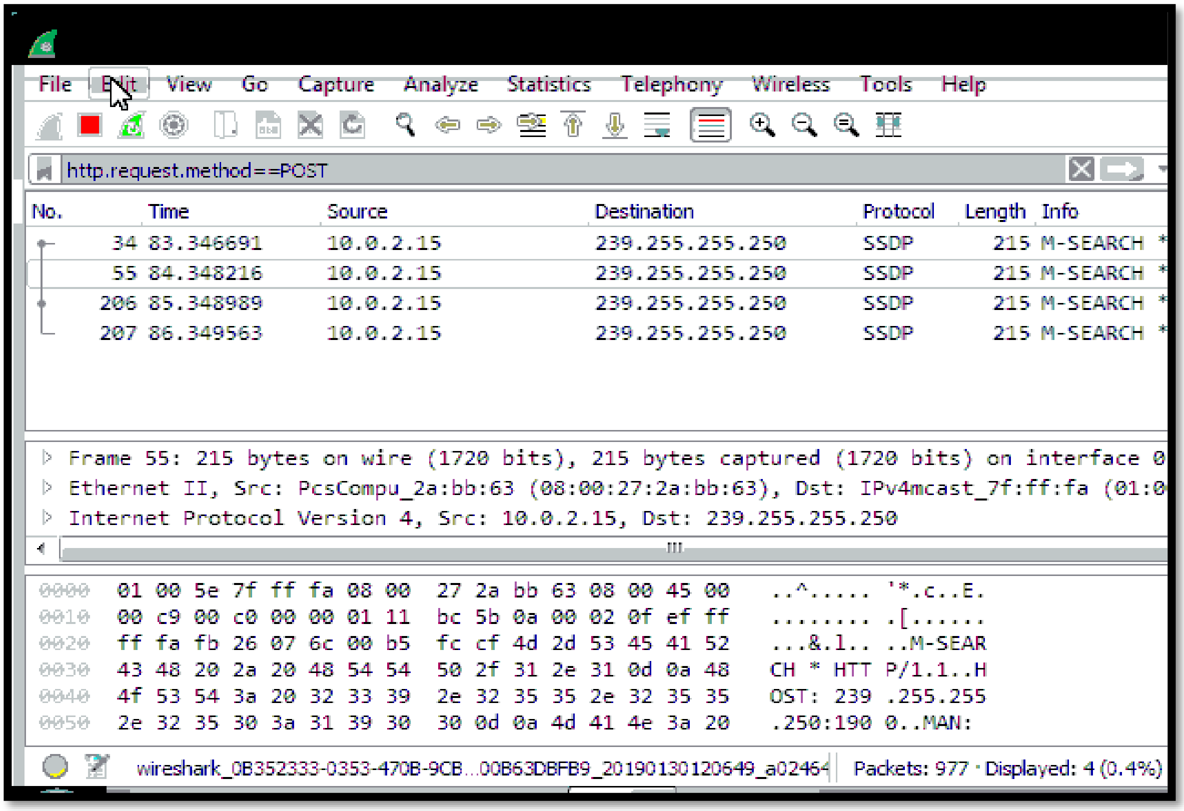
Frame (413 bytes)
Reassembled TCP (1779 bytes)
Transmission Control Protocol: Protocol
Packets: 90 · Displayed: 23 (25.6%)
Profile: Default

Eg:- tcp

- http.request Packets :-

It displays packets which are using http request.

Eg :- http.request.method==POST



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method==POST
```

```
No.    Time          Source       Destination        Protocol  Length  Info
   34  83.346691     10.0.2.15    239.255.255.250    SSDP      215     M-SEARCH *
   55  84.348216     10.0.2.15    239.255.255.250    SSDP      215     M-SEARCH *
  206  85.348989     10.0.2.15    239.255.255.250    SSDP      215     M-SEARCH *
  207  86.349563     10.0.2.15    239.255.255.250    SSDP      215     M-SEARCH *
```

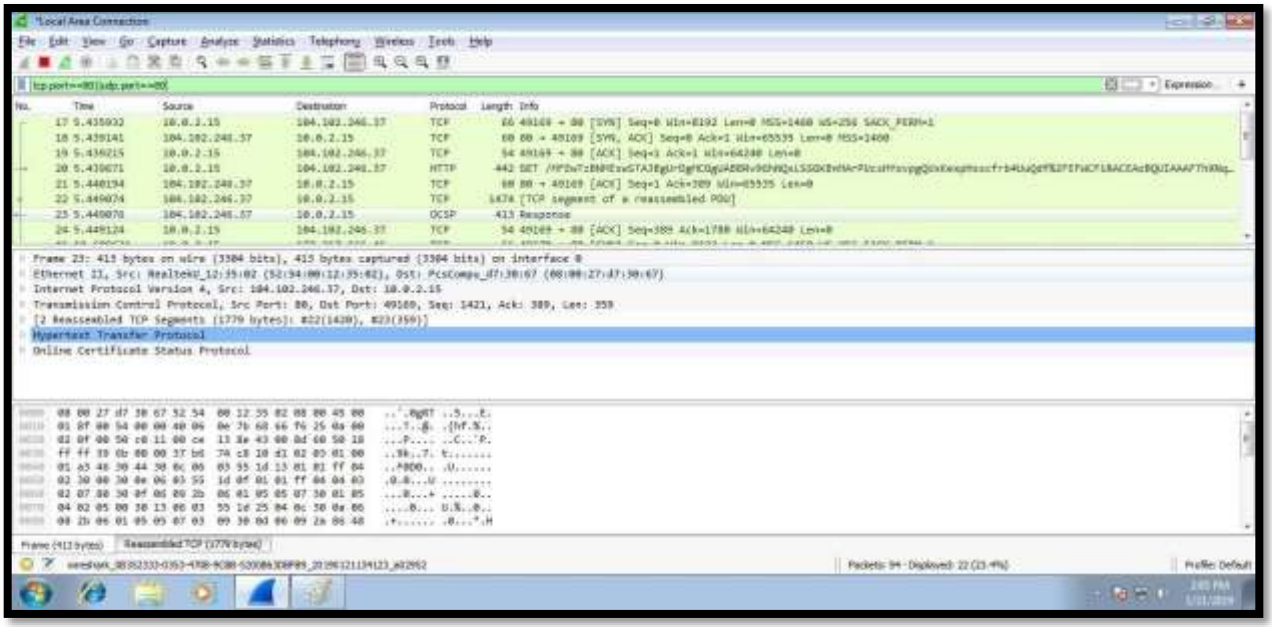
```
▷ Frame 55: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
▷ Ethernet II, Src: PcsCompu_2a:bb:63 (08:00:27:2a:bb:63), Dst: IPv4mcast_7f:ff:fa (01:0
▷ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 239.255.255.250
```

```
0000  01 00 5e 7f ff fa 08 00  27 2a bb 63 08 00 45 00   ..^..... '*.c..E.
0010  00 c9 00 c0 00 00 01 11  bc 5b 0a 00 02 0f ef ff   ........ .[......
0020  ff fa fb 26 07 6c 00 b5  fc cf 4d 2d 53 45 41 52   ...&.l.. ..M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1..H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0..MAN:
```

wireshark_0B352333-0353-470B-9CB…00B63DBFB9_20190130120649_a0246
Packets: 977 · Displayed: 4 (0.4%)

- TCP and UDP Packets :-
  To capture TCP & UDP packets on same port.

  Eg :- For Port 80 tcp.port ==80 || udp.port ==80

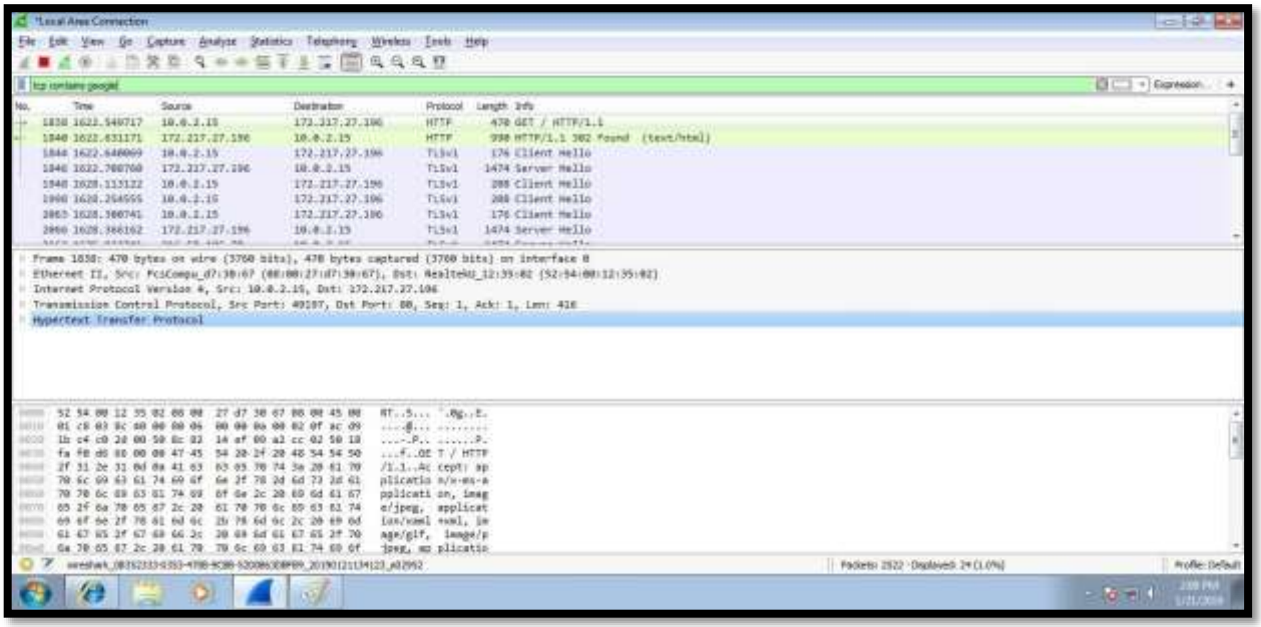

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
tcp.port==80||udp.port==80

No.  Time        Source          Destination     Protocol Length Info
  17 5.435932    10.0.2.15       104.102.246.37  TCP        66 49169 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  18 5.439141    104.102.246.37  10.0.2.15       TCP        60 80 → 49169 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
  19 5.439215    10.0.2.15       104.102.246.37  TCP        54 49169 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  20 5.439671    10.0.2.15       104.102.246.37  HTTP      442 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR[illegible]…
  21 5.440194    104.102.246.37  10.0.2.15       TCP        60 80 → 49169 [ACK] Seq=1 Ack=389 Win=65535 Len=0
  22 5.449074    104.102.246.37  10.0.2.15       TCP      1474 [TCP segment of a reassembled PDU]
  23 5.449078    104.102.246.37  10.0.2.15       OCSP      413 Response
  24 5.449124    10.0.2.15       104.102.246.37  TCP        54 49169 → 80 [ACK] Seq=389 Ack=1780 Win=64240 Len=0

Frame 23: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d7:30:67 (08:00:27:d7:30:67)
Internet Protocol Version 4, Src: 104.102.246.37, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 49169, Seq: 1421, Ack: 389, Len: 359
[2 Reassembled TCP Segments (1779 bytes): #22(1420), #23(359)]
Hypertext Transfer Protocol
Online Certificate Status Protocol

0000  08 00 27 d7 30 67 52 54  00 12 35 02 08 00 45 00   ..'.0gRT ..5...E.
0010  01 8f 00 54 00 00 40 06  0e 7b 68 66 f6 25 0a 00   ...T..@. .{hf.%..
0020  02 0f 00 50 c0 11 00 ce  13 8e 43 00 0d 60 50 18   ...P.... ..C..`P.
0030  ff ff 39 0b 00 00 37 b6  74 c8 10 d1 02 03 01 00   ..9...7. t.......
0040  01 a3 48 30 44 30 0c 06  03 55 1d 13 01 01 ff 04   ..H0D0.. .U......
0050  02 30 00 30 0e 06 03 55  1d 0f 01 01 ff 04 04 03   .0.0...U ........
0060  02 07 80 30 0f 06 09 2b  06 01 05 05 07 30 01 05   ...0...+ .....0..
0070  04 02 05 00 30 13 06 03  55 1d 25 04 0c 30 0a 06   ....0... U.%..0..
0080  08 2b 06 01 05 05 07 03  09 30 0d 06 09 2a 86 48   .+...... .0...*.H

Frame (413 bytes)   Reassembled TCP (1779 bytes)
wireshark_0B35233-0353-4788-9C88-52008630BF89_20190121134123_a02952    Packets: 94 · Displayed: 22 (23.4%)    Profile: Default
```

- Packets Containing Keyword :-

  It display packets which contain some keyword.

  Eg :- For Google tcp contains google

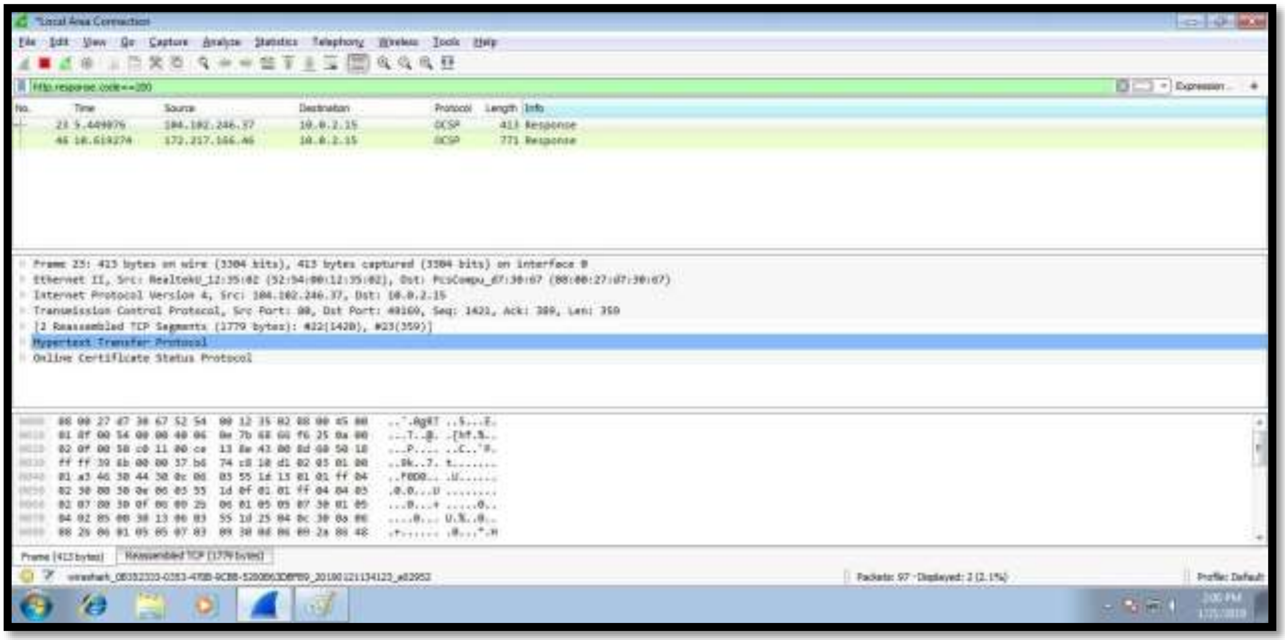

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
tcp contains google

No.  Time           Source          Destination     Protocol Length Info
1838 1622.549717    10.0.2.15       172.217.27.196  HTTP      470 GET / HTTP/1.1
1840 1622.631171    172.217.27.196  10.0.2.15       HTTP      998 HTTP/1.1 302 Found  (text/html)
1844 1622.640069    10.0.2.15       172.217.27.196  TLSv1     176 Client Hello
1846 1622.700700    172.217.27.196  10.0.2.15       TLSv1    1474 Server Hello
1948 1628.113122    10.0.2.15       172.217.27.196  TLSv1     208 Client Hello
1960 1628.254555    10.0.2.15       172.217.27.196  TLSv1     208 Client Hello
2063 1628.300741    10.0.2.15       172.217.27.196  TLSv1     176 Client Hello
2066 1628.366162    172.217.27.196  10.0.2.15       TLSv1    1474 Server Hello

Frame 1838: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
Ethernet II, Src: PcsCompu_d7:30:67 (08:00:27:d7:30:67), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.217.27.196
Transmission Control Protocol, Src Port: 49187, Dst Port: 80, Seq: 1, Ack: 1, Len: 416
Hypertext Transfer Protocol

0000  52 54 00 12 35 02 08 00  27 d7 30 67 08 00 45 00   RT..5... '.0g..E.
0010  01 c8 03 8c 40 00 80 06  00 00 0a 00 02 0f ac d9   ....@... ........
0020  1b c4 c0 23 00 50 8c 82  14 af 00 a2 cc 02 50 18   ...#.P.. ......P.
0030  fa f0 d6 88 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 61 70   /1.1..Ac cept: ap
0050  70 6c 69 63 61 74 69 6f  6e 2f 78 2d 6d 73 2d 61   plicatio n/x-ms-a
0060  70 70 6c 69 63 61 74 69  6f 6e 2c 20 69 6d 61 67   pplicati on, imag
0070  65 2f 6a 70 65 67 2c 20  61 70 70 6c 69 63 61 74   e/jpeg,  applicat
0080  69 6f 6e 2f 78 61 6d 6c  2b 78 6d 6c 2c 20 69 6d   ion/xaml +xml, im
0090  61 67 65 2f 67 69 66 2c  20 69 6d 61 67 65 2f 70   age/gif,  image/p
00a0  6a 70 65 67 2c 20 61 70  70 6c 69 63 61 74 69 6f   jpeg, ap plicatio

wireshark_0B35233-0353-4788-9C88-52008630BF89_20190121134123_a02952    Packets: 2522 · Displayed: 24 (1.0%)    Profile: Default
```

- http.response Packets :-

It displays packets having number of errors connecting to server.

Eg :- http.response.code ==200


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
http.response.code==200
```

```
No.   Time          Source           Destination   Protocol  Length  Info
   23 5.449876      104.102.246.37   10.0.2.15     OCSP         413  Response
   46 10.619274     172.217.166.46   10.0.2.15     OCSP         771  Response
```

```
Frame 23: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_d7:30:67 (08:00:27:d7:30:67)
Internet Protocol Version 4, Src: 104.102.246.37, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 49169, Seq: 1421, Ack: 389, Len: 359
[2 Reassembled TCP Segments (1779 bytes): #22(1420), #23(359)]
Hypertext Transfer Protocol
Online Certificate Status Protocol
```

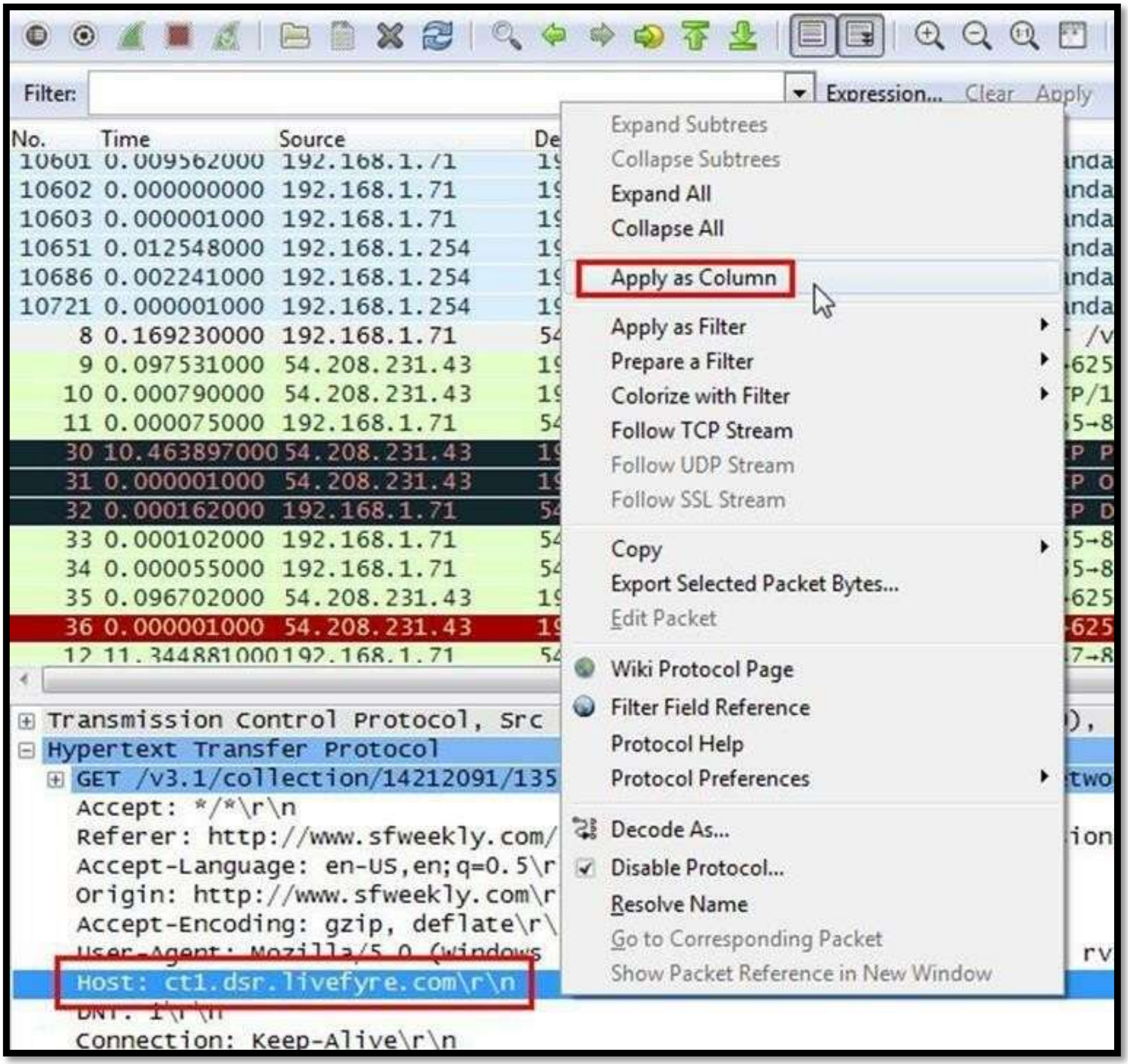
```
0000  08 00 27 d7 30 67 52 54  00 12 35 02 08 00 45 00   ..'.0gRT ..5...E.
0010  01 8f 00 54 00 00 40 06  0e 7b 68 66 f6 25 0a 00   ...T..@. .{hf.%..
0020  02 0f 00 50 c0 11 00 ce  13 8e 43 00 8d 60 50 18   ...P.... ..C..`P.
0030  ff ff 39 6b 00 00 37 b6  74 c8 10 d1 02 03 01 00   ..9k..7. t.......
0040  01 a3 46 30 44 30 0c 06  03 55 1d 13 01 01 ff 04   ..F0D0.. .U......
0050  02 30 00 30 0e 06 03 55  1d 0f 01 01 ff 04 04 03   .0.0...U ........
0060  02 07 80 30 0f 06 00 2b  06 01 05 05 07 30 01 05   ...0...+ .....0..
0070  04 02 05 00 30 13 06 03  55 1d 25 04 0c 30 0a 06   ....0... U.%..0..
0080  08 2b 06 01 05 05 07 03  09 30 0d 06 09 2a 86 48   .+...... .0...*.H
```

Frame (413 bytes)
Reassembled TCP (1779 bytes)
wireshark_0B352333-0353-470B-9CB8-5200863D8F89_20180121134123_a02952
Packets: 97 · Displayed: 2 (2.1%)
Profile: Default

AIM: Analyze the packets provided in lab and solve the questions using Wireshark

1. What web server software issued by www.snopes.com?

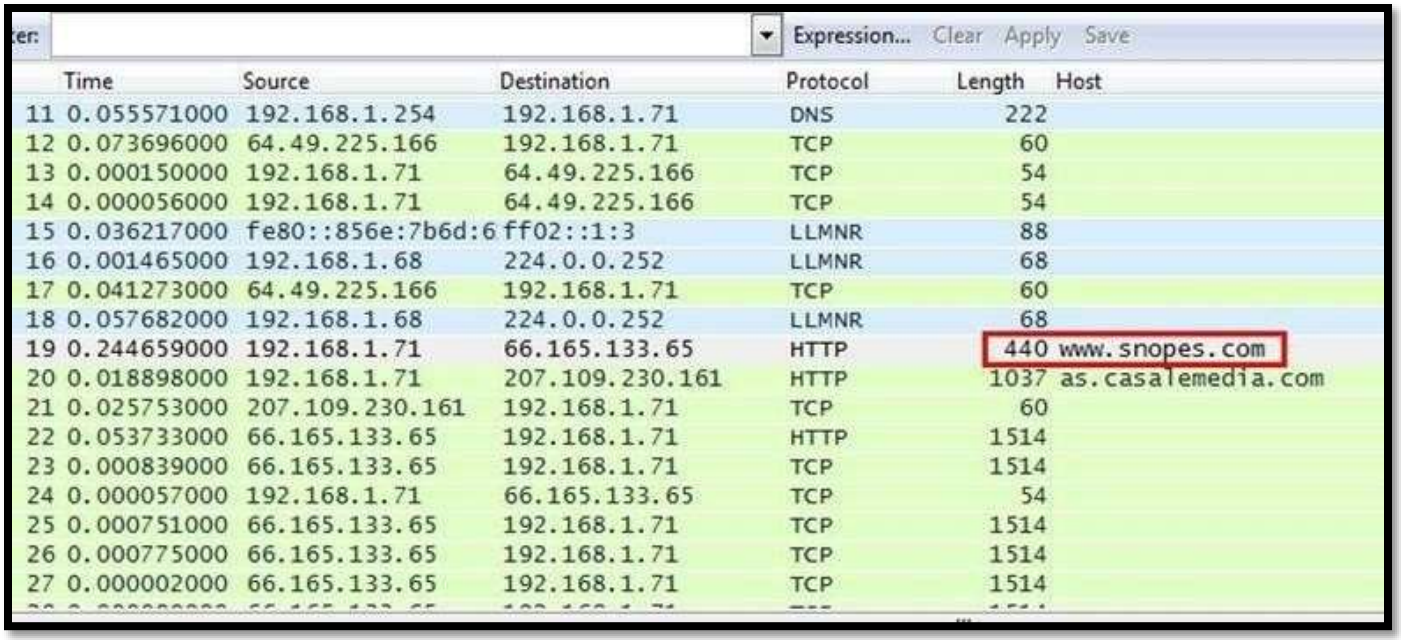
Analysis – The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column.



```
No.     Time          Source           De
10601 0.009562000 192.168.1.71     19                nda
10602 0.000000000 192.168.1.71     19                nda
10603 0.000001000 192.168.1.71     19                nda
10651 0.012548000 192.168.1.254    19                nda
10686 0.002241000 192.168.1.254    19                nda
10721 0.000001000 192.168.1.254    19                nda
    8 0.169230000 192.168.1.71     54                 /v
    9 0.097531000 54.208.231.43    19                625
   10 0.000790000 54.208.231.43    19                P/1
   11 0.000075000 192.168.1.71     54                5→8
   30 10.463897000 54.208.231.43   19                P P
   31 0.000001000 54.208.231.43    19                P O
   32 0.000162000 192.168.1.71     54                P D
   33 0.000102000 192.168.1.71     54                5→8
   34 0.000055000 192.168.1.71     54                5→8
   35 0.096702000 54.208.231.43    19                625
   36 0.000001000 54.208.231.43    19                625
   12 11.344881000 192.168.1.71    54                7→8
```

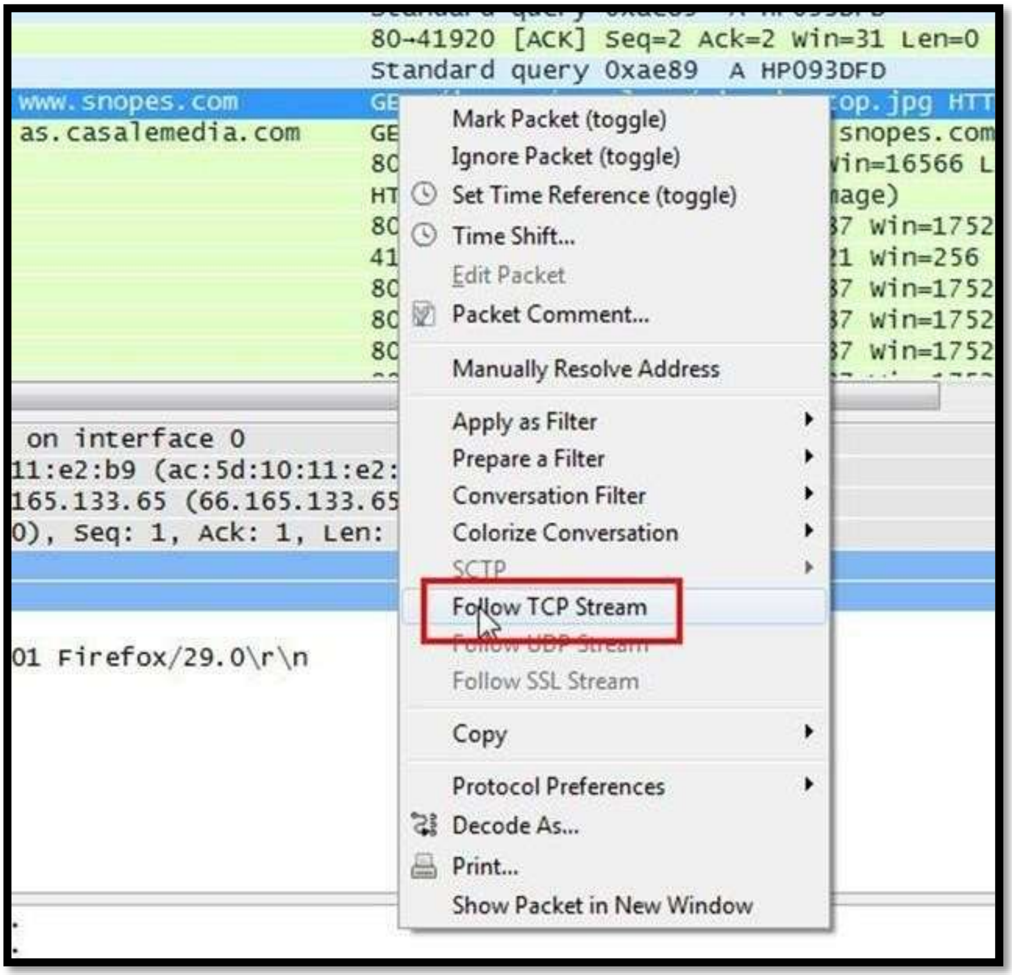
```
⊞ Transmission Control Protocol, Src                 ),
⊟ Hypertext Transfer Protocol
  ⊞ GET /v3.1/collection/14212091/135                two
    Accept: */*\r\n
    Referer: http://www.sfweekly.com/                ion
    Accept-Language: en-US,en;q=0.5\r
    Origin: http://www.sfweekly.com\r
    Accept-Encoding: gzip, deflate\r\
    User-Agent: Mozilla/5.0 (Windows                 rv
    Host: ct1.dsr.livefyre.com\r\n
    DNT: 1\r\n
    Connection: Keep-Alive\r\n
```

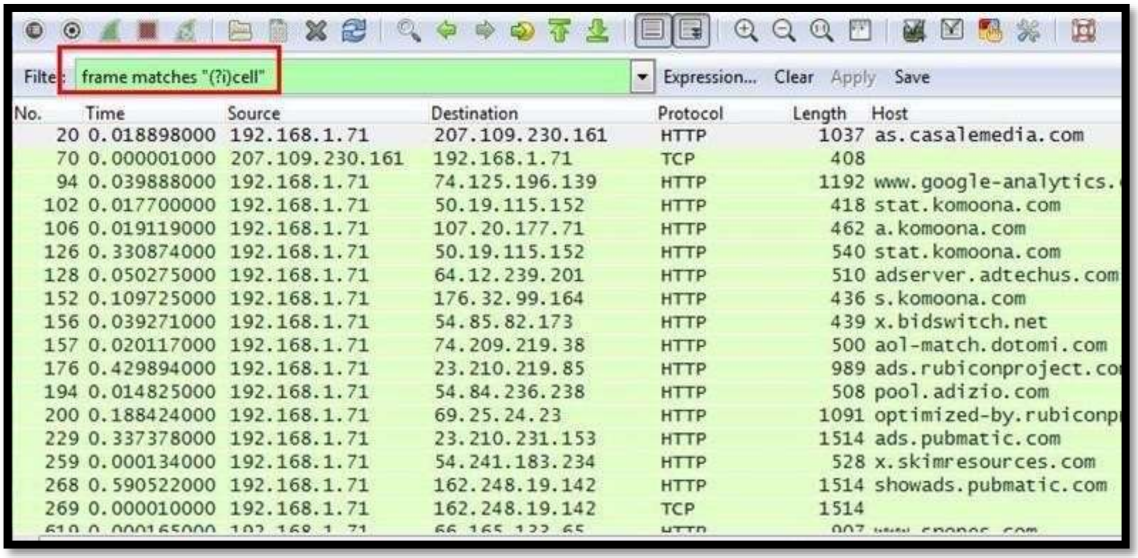
Now we can see our host www.snopes.com in host column.



	Time	Source	Destination	Protocol	Length	Host
11	0.055571000	192.168.1.254	192.168.1.71	DNS	222	
12	0.073696000	64.49.225.166	192.168.1.71	TCP	60	
13	0.000150000	192.168.1.71	64.49.225.166	TCP	54	
14	0.000056000	192.168.1.71	64.49.225.166	TCP	54	
15	0.036217000	fe80::856e:7b6d:6	ff02::1:3	LLMNR	88	
16	0.001465000	192.168.1.68	224.0.0.252	LLMNR	68	
17	0.041273000	64.49.225.166	192.168.1.71	TCP	60	
18	0.057682000	192.168.1.68	224.0.0.252	LLMNR	68	
19	0.244659000	192.168.1.71	66.165.133.65	HTTP	440	www.snopes.com
20	0.018898000	192.168.1.71	207.109.230.161	HTTP	1037	as.casalemedia.com
21	0.025753000	207.109.230.161	192.168.1.71	TCP	60	
22	0.053733000	66.165.133.65	192.168.1.71	HTTP	1514	
23	0.000839000	66.165.133.65	192.168.1.71	TCP	1514	
24	0.000057000	192.168.1.71	66.165.133.65	TCP	54	
25	0.000751000	66.165.133.65	192.168.1.71	TCP	1514	
26	0.000775000	66.165.133.65	192.168.1.71	TCP	1514	
27	0.000002000	66.165.133.65	192.168.1.71	TCP	1514	

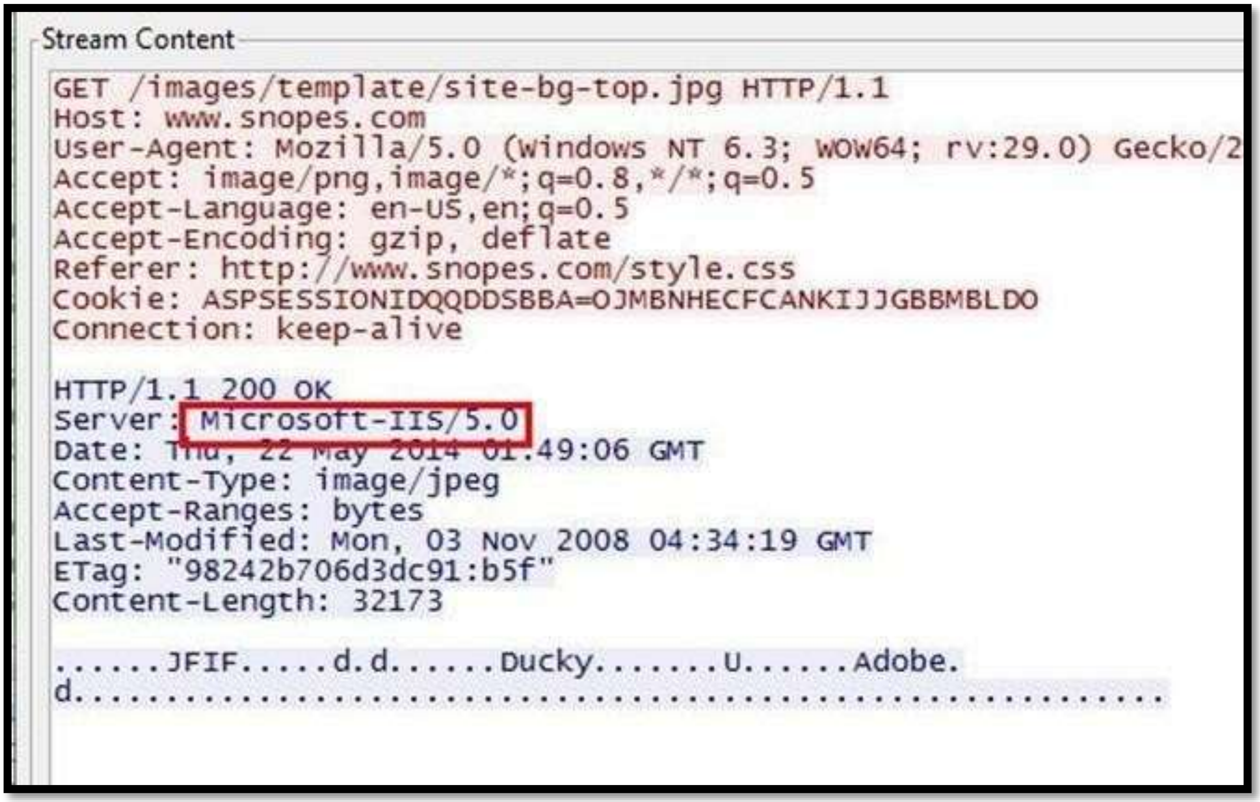
Right click on the selected packet and then select Follow TCP stream.


```
                        80→41920 [ACK] Seq=2 Ack=2 Win=31 Len=0
                        Standard query 0xae89  A HP093DFD
www.snopes.com          GE                           op.jpg HTT
as.casalemedia.com      GE                           snopes.com
                        80                           Win=16566 L
                        HT                           age)
                        80                           7 Win=1752
                        41                           1 Win=256
                        80                           7 Win=1752
                        80                           7 Win=1752
                        80                           7 Win=1752

 on interface 0
11:e2:b9 (ac:5d:10:11:e2:
165.133.65 (66.165.133.65
0), Seq: 1, Ack: 1, Len:

01 Firefox/29.0\r\n
```



```
Filter: frame matches "(?i)cell"

No.   Time        Source           Destination      Protocol  Length Host
   20 0.018898000 192.168.1.71     207.109.230.161  HTTP      1037 as.casalemedia.com
   70 0.000001000 207.109.230.161  192.168.1.71     TCP        408
   94 0.039888000 192.168.1.71     74.125.196.139   HTTP      1192 www.google-analytics.
  102 0.017700000 192.168.1.71     50.19.115.152    HTTP       418 stat.komoona.com
  106 0.019119000 192.168.1.71     107.20.177.71    HTTP       462 a.komoona.com
  126 0.330874000 192.168.1.71     50.19.115.152    HTTP       540 stat.komoona.com
  128 0.050275000 192.168.1.71     64.12.239.201    HTTP       510 adserver.adtechus.com
  152 0.109725000 192.168.1.71     176.32.99.164    HTTP       436 s.komoona.com
  156 0.039271000 192.168.1.71     54.85.82.173     HTTP       439 x.bidswitch.net
  157 0.020117000 192.168.1.71     74.209.219.38    HTTP       500 aol-match.dotomi.com
  176 0.429894000 192.168.1.71     23.210.219.85    HTTP       989 ads.rubiconproject.co
  194 0.014825000 192.168.1.71     54.84.236.238    HTTP       508 pool.adizio.com
  200 0.188424000 192.168.1.71     69.25.24.23      HTTP      1091 optimized-by.rubiconp
  229 0.337378000 192.168.1.71     23.210.231.153   HTTP      1514 ads.pubmatic.com
  259 0.000134000 192.168.1.71     54.241.183.234   HTTP       528 x.skimresources.com
  268 0.590522000 192.168.1.71     162.248.19.142   HTTP      1514 showads.pubmatic.com
  269 0.000010000 192.168.1.71     162.248.19.142   TCP       1514
  619 0.000165000 192.168.1.71     66.165.133.65    HTTP       907 www.snopes.com
```

Now we can see the webserver name in server header it is Microsoft IIS 5.0

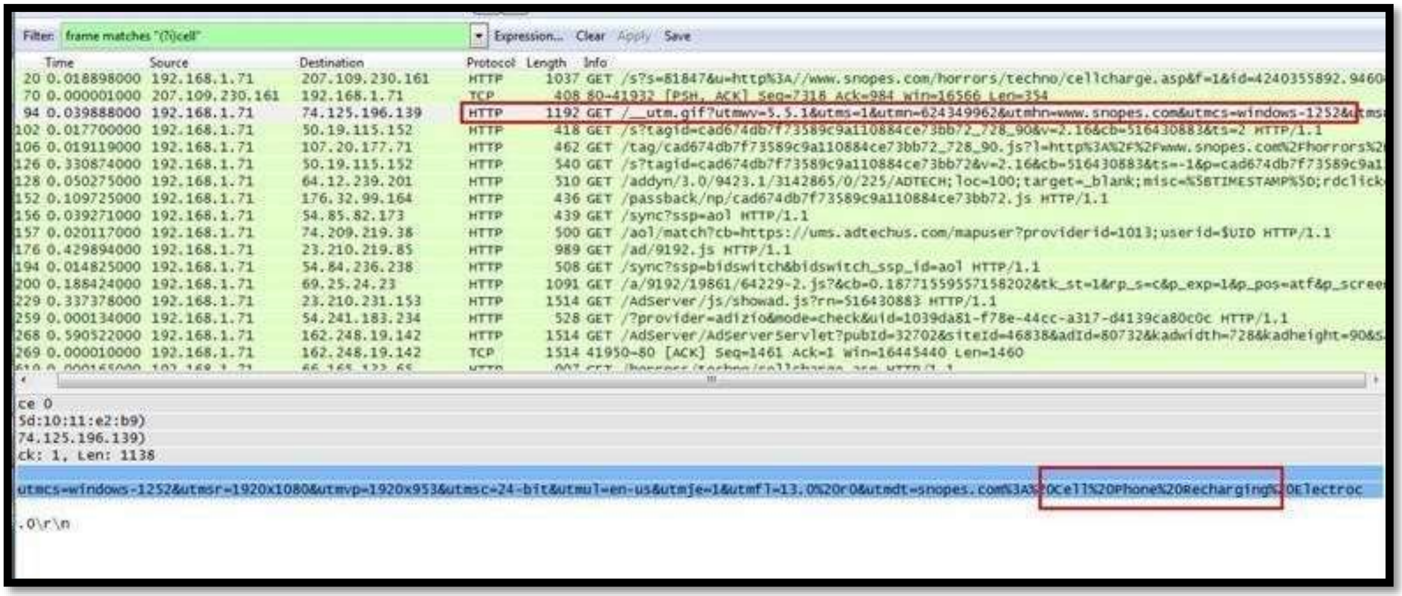


```
GET /images/template/site-bg-top.jpg HTTP/1.1
Host: www.snopes.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/2
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.snopes.com/style.css
Cookie: ASPSESSIONIDQQDDSBBA=OJMBNHECFCANKIJJGBBMBLDO
Connection: keep-alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 22 May 2014 01:49:06 GMT
Content-Type: image/jpeg
Accept-Ranges: bytes
Last-Modified: Mon, 03 Nov 2008 04:34:19 GMT
ETag: "98242b706d3dc91:b5f"
Content-Length: 32173

......JFIF.....d.d......Ducky.......U......Adobe.
d............................................................
```

2. About what cell phone problem is the client concerned?

Analysis – Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches "(?!) cell"

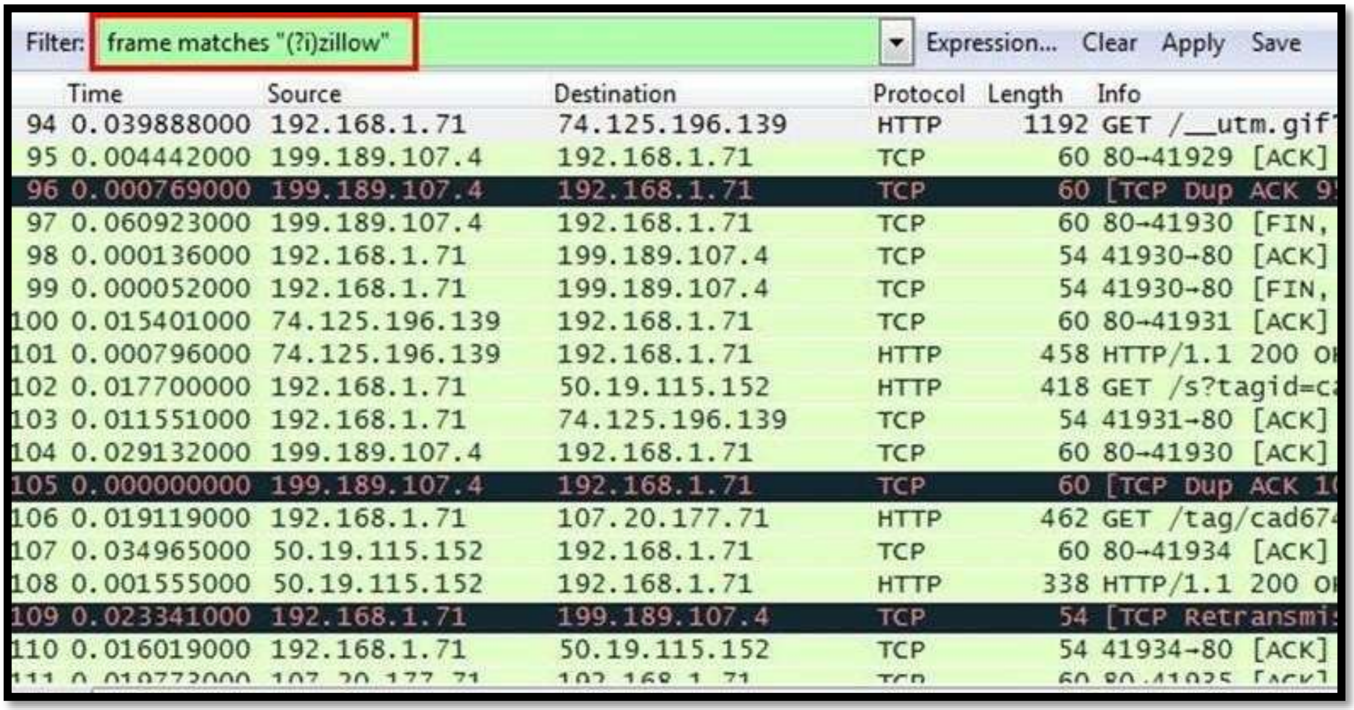
After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request cell keyword is in URL and it was about cell phone charging issue.



```
Filter: frame matches "(?i)cell"                    Expression... Clear Apply Save
     Time          Source            Destination       Protocol Length Info
 20 0.018898000 192.168.1.71       207.109.230.161    HTTP     1037 GET /s?s=81847&u=http%3A//www.snopes.com/horrors/techno/cellcharge.asp&f=1&id=4240355892.9460
 70 0.000001000 207.109.230.161    192.168.1.71       TCP       408 80→41932 [PSH, ACK] Seq=7318 Ack=984 Win=16566 Len=354
 94 0.039888000 192.168.1.71       74.125.196.139     HTTP     1192 GET /__utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs=windows-1252&utms
102 0.017700000 192.168.1.71       50.19.115.152      HTTP      418 GET /s?tagid=cad674db7f73589c9a110884ce73bb72_728_90&v=2.16&cb=516430883&ts=2 HTTP/1.1
106 0.019119000 192.168.1.71       107.20.177.71      HTTP      462 GET /tag/cad674db7f73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%2Fhorrors%2
126 0.330874000 192.168.1.71       50.19.115.152      HTTP      540 GET /s?tagid=cad674db7f73589c9a110884ce73bb72&v=2.16&cb=516430883&ts=-1&p=cad674db7f73589c9a1
128 0.050275000 192.168.1.71       64.12.239.201      HTTP      510 GET /addyn/3.0/9423.1/3142865/0/225/ADTECH;loc=100;target=_blank;misc=%5BTIMESTAMP%5D;rdclick
152 0.109725000 192.168.1.71       176.32.99.164      HTTP      436 GET /passback/np/cad674db7f73589c9a110884ce73bb72.js HTTP/1.1
156 0.039271000 192.168.1.71       54.85.82.173       HTTP      439 GET /sync?ssp=aol HTTP/1.1
157 0.020117000 192.168.1.71       74.209.219.38      HTTP      500 GET /aol/match?cb=https://ums.adtechus.com/mapuser?providerid=1013;userid=$UID HTTP/1.1
176 0.429894000 192.168.1.71       23.210.219.85      HTTP      989 GET /ad/9192.js HTTP/1.1
194 0.014825000 192.168.1.71       54.84.236.238      HTTP      508 GET /sync?ssp=bidswitch&bidswitch_ssp_id=aol HTTP/1.1
200 0.188424000 192.168.1.71       69.25.24.23        HTTP     1091 GET /a/9192/19861/64229-2.js?&cb=0.18771559557158202&tk_st=1&rp_s=c&p_exp=1&p_pos=atf&p_scree
229 0.337378000 192.168.1.71       23.210.231.153     HTTP     1514 GET /AdServer/js/showad.js?rn=516430883 HTTP/1.1
259 0.000134000 192.168.1.71       54.241.183.234     HTTP      528 GET /?provider=adizio&mode=check&uid=1039da81-f78e-44cc-a317-d4139ca80c0c HTTP/1.1
268 0.590522000 192.168.1.71       162.248.19.142     HTTP     1514 GET /AdServer/AdServerServlet?pubId=32702&siteId=46838&adId=80732&kadwidth=728&kadheight=90&S
269 0.000010000 192.168.1.71       162.248.19.142     TCP      1514 41950→80 [ACK] Seq=1461 Ack=1 Win=16445440 Len=1460
610 0.000165000 192.168.1.71       66.165.133.65      HTTP      907 GET /horrors/techno/cellcharge.asp HTTP/1.1

ce 0
5d:10:11:e2:b9)
74.125.196.139)
ck: 1, Len: 1138

utmcs=windows-1252&utmsr=1920x1080&utmvp=1920x953&utmsc=24-bit&utmul=en-us&utmje=1&utmfl=13.0%20r0&utmdt=snopes.com%3A%20Cell%20Phone%20Recharging%20Electroc

.0\r\n
```

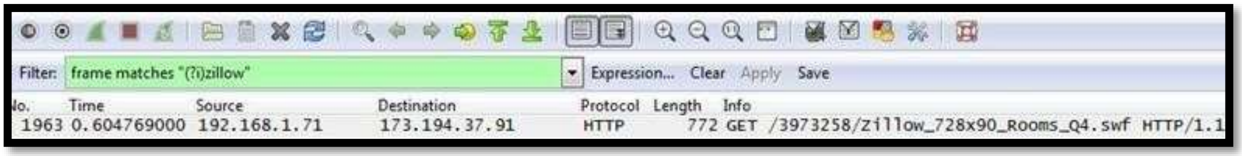
3. According to Zillow, what instrument will Ryan learn to play?

Analysis – As we did in the last challenge, we will apply a regular express filter for the Zillow keyword. Apply frame matched “(?!) zillow”



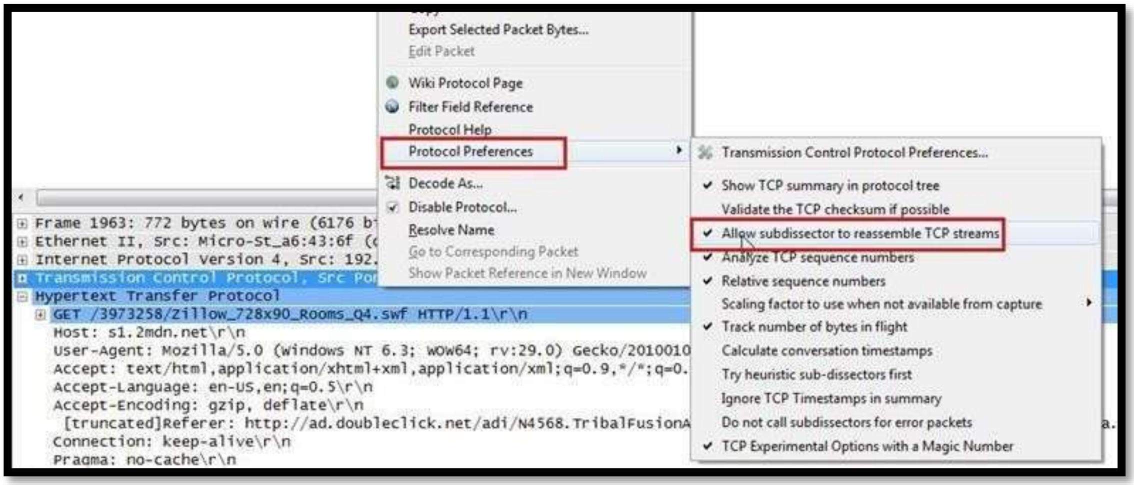
```
Filter: frame matches "(?i)zillow"                  Expression... Clear Apply Save
     Time         Source           Destination      Protocol Length Info
 94 0.039888000 192.168.1.71     74.125.196.139   HTTP     1192 GET /__utm.gif
 95 0.004442000 199.189.107.4    192.168.1.71     TCP        60 80→41929 [ACK]
 96 0.000769000 199.189.107.4    192.168.1.71     TCP        60 [TCP Dup ACK 9
 97 0.060923000 199.189.107.4    192.168.1.71     TCP        60 80→41930 [FIN,
 98 0.000136000 192.168.1.71     199.189.107.4    TCP        54 41930→80 [ACK]
 99 0.000052000 192.168.1.71     199.189.107.4    TCP        54 41930→80 [FIN,
100 0.015401000 74.125.196.139   192.168.1.71     TCP        60 80→41931 [ACK]
101 0.000796000 74.125.196.139   192.168.1.71     HTTP      458 HTTP/1.1 200 OK
102 0.017700000 192.168.1.71     50.19.115.152    HTTP      418 GET /s?tagid=ca
103 0.011551000 192.168.1.71     74.125.196.139   TCP        54 41931→80 [ACK]
104 0.029132000 199.189.107.4    192.168.1.71     TCP        60 80→41930 [ACK]
105 0.000000000 199.189.107.4    192.168.1.71     TCP        60 [TCP Dup ACK 1
106 0.019119000 192.168.1.71     107.20.177.71    HTTP      462 GET /tag/cad67
107 0.034965000 50.19.115.152    192.168.1.71     TCP        60 80→41934 [ACK]
108 0.001555000 50.19.115.152    192.168.1.71     HTTP      338 HTTP/1.1 200 OK
109 0.023341000 192.168.1.71     199.189.107.4    TCP        54 [TCP Retransmi
110 0.016019000 192.168.1.71     50.19.115.152    TCP        54 41934→80 [ACK]
111 0.010773000 107.20.177.71    192.168.1.71     TCP        60 80→41935 [ACK]
```

After applying the filter, we found only one packet with the Zillow keyword



```
Filter: frame matches "(?i)zillow"                  Expression... Clear Apply Save
No.  Time        Source          Destination      Protocol Length Info
1963 0.604769000 192.168.1.71    173.194.37.91    HTTP      772 GET /3973258/Zillow_728x90_Rooms_Q4.swf HTTP/1.1
```

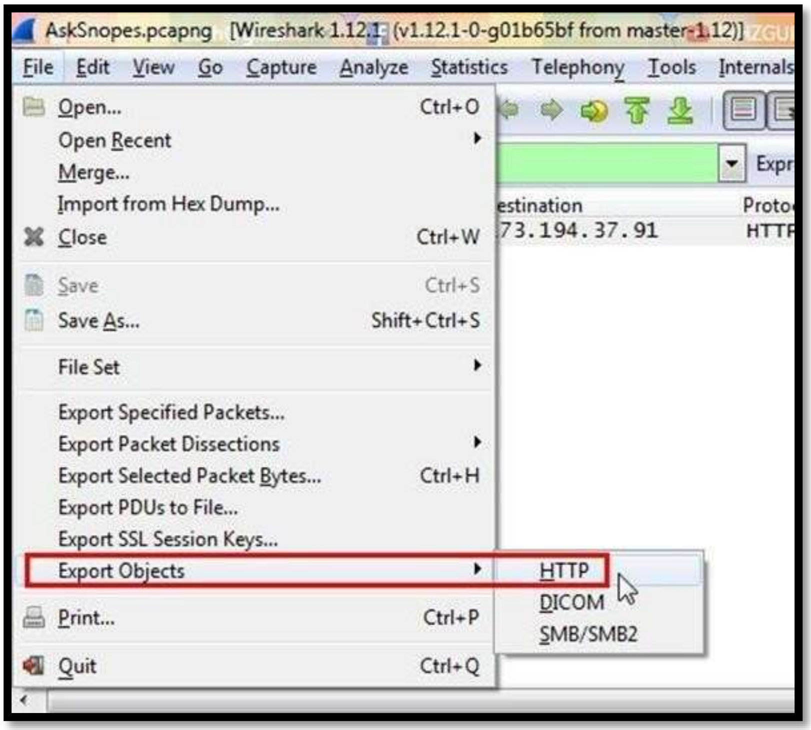
Select the packet and expand the Hypertext Transfer Protocol tab right click on it go to Protocol Preferences and check Allow subdissector to resemble TCP stream.


Export Selected Packet Bytes...
Edit Packet
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
Show Packet Reference in New Window
Transmission Control Protocol Preferences...

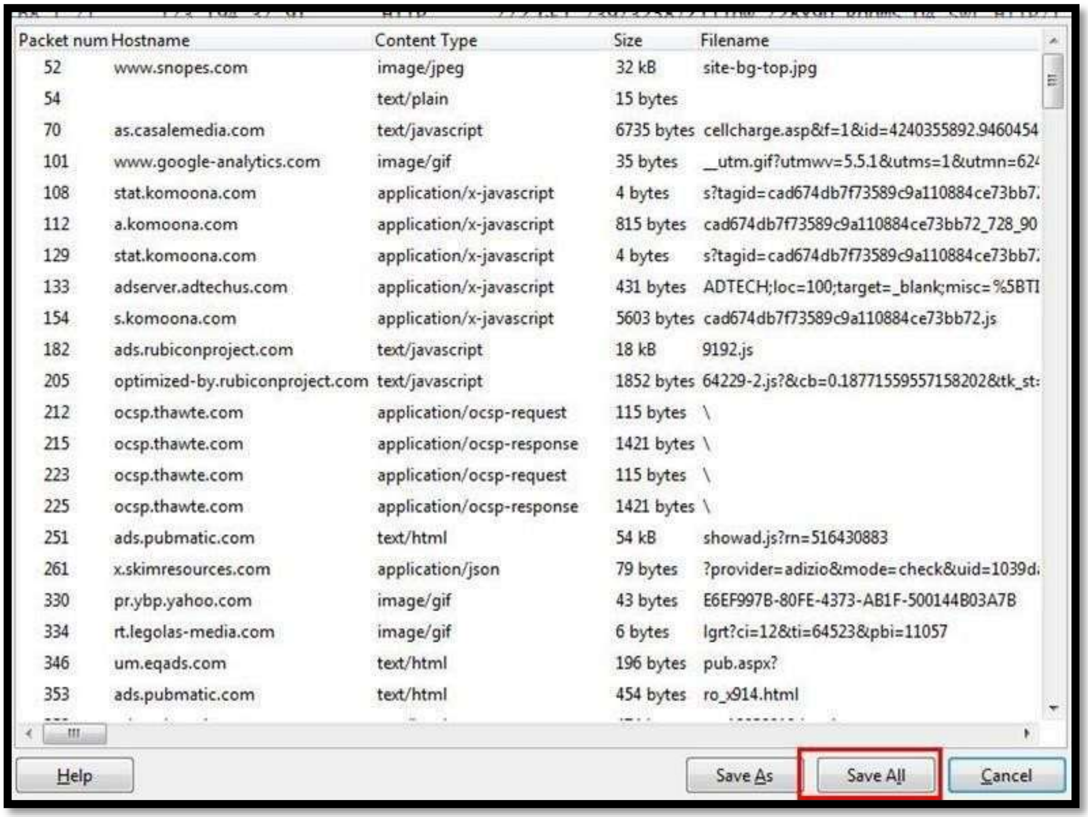
```
⊞ Frame 1963: 772 bytes on wire (6176 b
⊞ Ethernet II, Src: Micro-St_a6:43:6f (c
⊞ Internet Protocol Version 4, Src: 192.
⊞ Transmission Control Protocol, Src Por
⊟ Hypertext Transfer Protocol
  ⊞ GET /3973258/Zillow_728x90_Rooms_Q4.swf HTTP/1.1\r\n
    Host: s1.2mdn.net\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:29.0) Gecko/2010010
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
     [truncated]Referer: http://ad.doubleclick.net/adi/N4568.TribalFusionA
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
```

✓ Show TCP summary in protocol tree
Validate the TCP checksum if possible
✓ Allow subdissector to reassemble TCP streams
✓ Analyze TCP sequence numbers
✓ Relative sequence numbers
Scaling factor to use when not available from capture
✓ Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
✓ TCP Experimental Options with a Magic Number

Now go to file and select Export Objects > HTTP. It will save all objects from the packet.

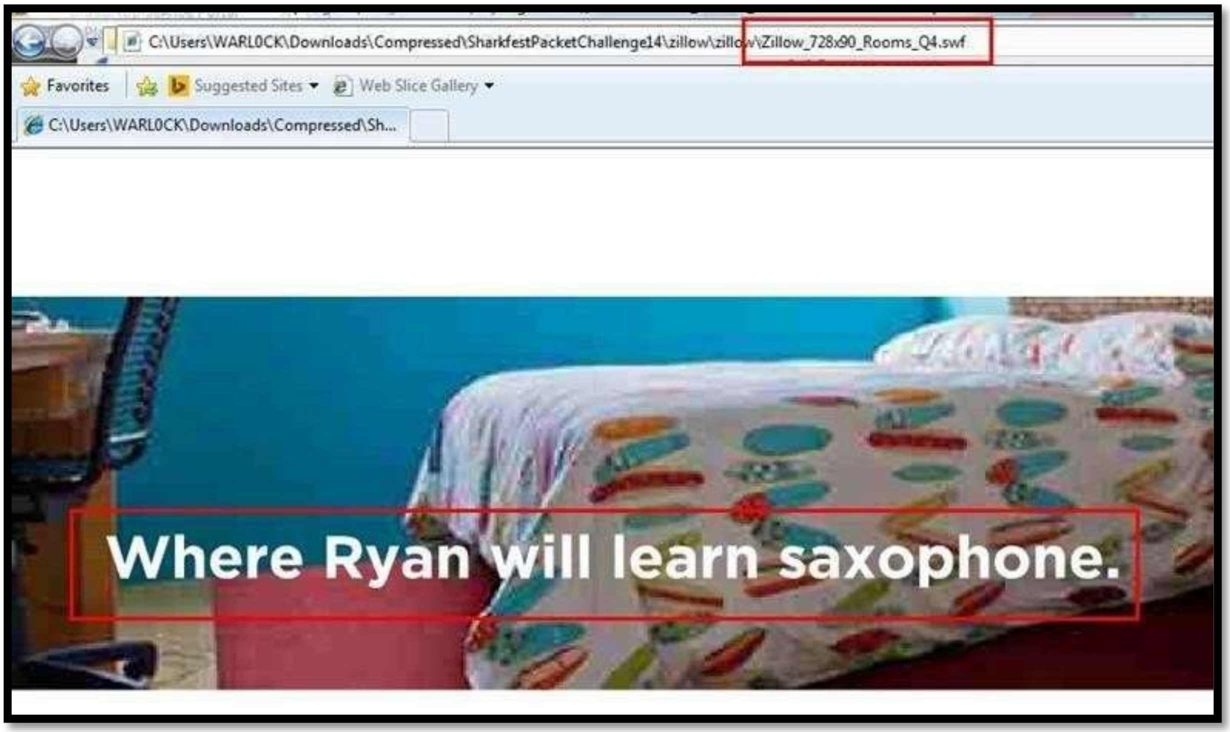


Click on save all.



Packet num	Hostname	Content Type	Size	Filename
52	www.snopes.com	image/jpeg	32 kB	site-bg-top.jpg
54		text/plain	15 bytes	
70	as.casalemedia.com	text/javascript	6735 bytes	cellcharge.asp&f=1&id=4240355892.9460454
101	www.google-analytics.com	image/gif	35 bytes	__utm.gif?utmwv=5.5.1&utms=1&utmn=62
108	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7
112	a.komoona.com	application/x-javascript	815 bytes	cad674db7f73589c9a110884ce73bb72_728_90
129	stat.komoona.com	application/x-javascript	4 bytes	s?tagid=cad674db7f73589c9a110884ce73bb7
133	adserver.adtechus.com	application/x-javascript	431 bytes	ADTECH;loc=100;target=_blank;misc=%5BTI
154	s.komoona.com	application/x-javascript	5603 bytes	cad674db7f73589c9a110884ce73bb72.js
182	ads.rubiconproject.com	text/javascript	18 kB	9192.js
205	optimized-by.rubiconproject.com	text/javascript	1852 bytes	64229-2.js?&cb=0.18771559557158202&tk_st
212	ocsp.thawte.com	application/ocsp-request	115 bytes	\
215	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
223	ocsp.thawte.com	application/ocsp-request	115 bytes	\
225	ocsp.thawte.com	application/ocsp-response	1421 bytes	\
251	ads.pubmatic.com	text/html	54 kB	showad.js?rn=516430883
261	x.skimresources.com	application/json	79 bytes	?provider=adizio&mode=check&uid=1039d
330	pr.ybp.yahoo.com	image/gif	43 bytes	E6EF997B-80FE-4373-AB1F-500144B03A7B
334	rt.legolas-media.com	image/gif	6 bytes	lgrt?ci=12&ti=64523&pbi=11057
346	um.eqads.com	text/html	196 bytes	pub.aspx?
353	ads.pubmatic.com	text/html	454 bytes	ro_x914.html

Help
Save As
Save All
Cancel



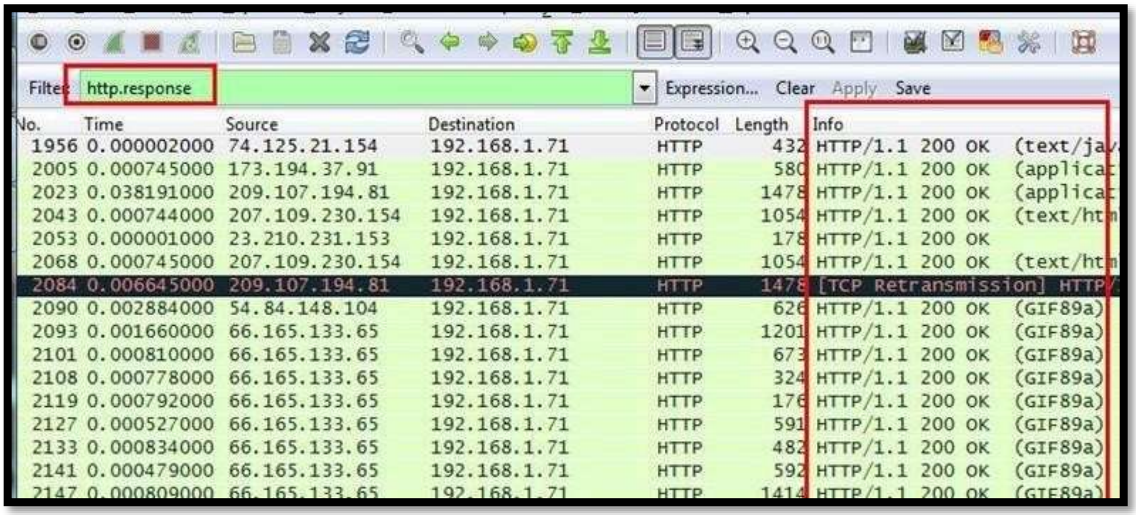
C:\Users\WARLOCK\Downloads\Compressed\SharkfestPacketChallenge14\zillow\zillow\Zillow_728x90_Rooms_Q4.swf

Favorites
Suggested Sites
Web Slice Gallery
C:\Users\WARLOCK\Downloads\Compressed\Sh...
Where Ryan will learn saxophone.

After saving all files in a directory and we found a swf file with name Zillow. After opening the flash file, we saw that Zillow was trying to learn saxophone.

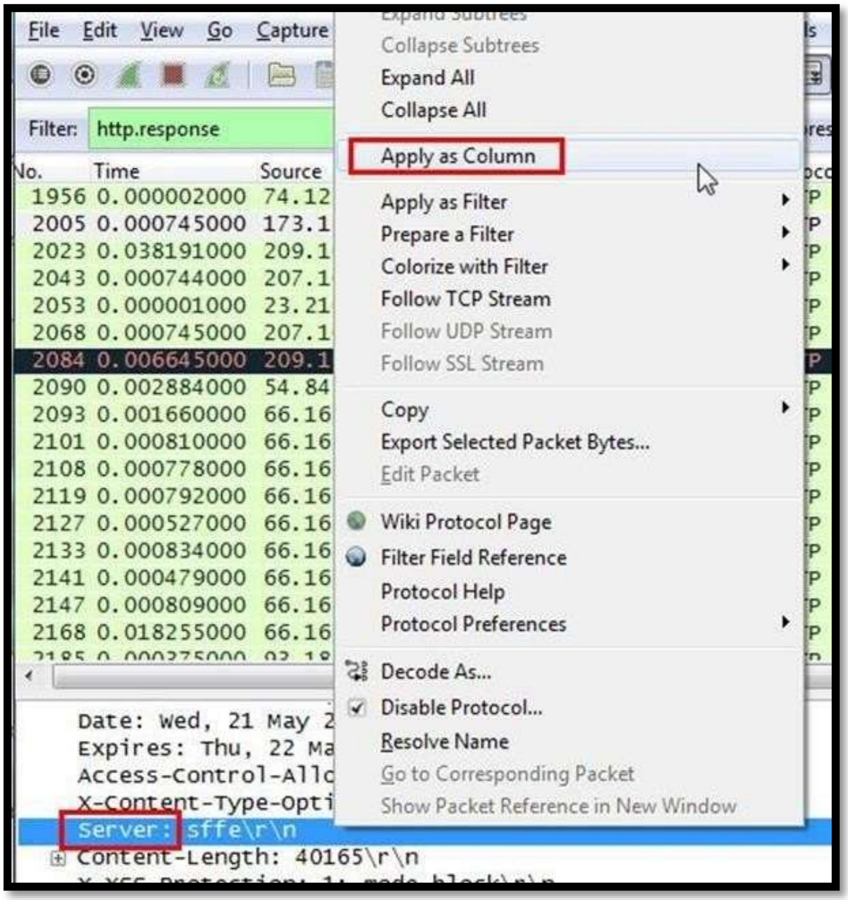
4. How many web servers are running Apache?

Analysis – The web server name can be retrieved from HTTP response header. So will apply filter http. response and we can see all http response packets.



```
Filter: http.response                      Expression...  Clear  Apply  Save
No.  Time        Source          Destination   Protocol Length Info
1956 0.000002000 74.125.21.154   192.168.1.71  HTTP     432  HTTP/1.1 200 OK  (text/ja
2005 0.000745000 173.194.37.91   192.168.1.71  HTTP     580  HTTP/1.1 200 OK  (applica
2023 0.038191000 209.107.194.81  192.168.1.71  HTTP     1478 HTTP/1.1 200 OK  (applica
2043 0.000744000 207.109.230.154 192.168.1.71  HTTP     1054 HTTP/1.1 200 OK  (text/ht
2053 0.000001000 23.210.231.153  192.168.1.71  HTTP     178  HTTP/1.1 200 OK
2068 0.000745000 207.109.230.154 192.168.1.71  HTTP     1054 HTTP/1.1 200 OK  (text/ht
2084 0.006645000 209.107.194.81  192.168.1.71  HTTP     1478 [TCP Retransmission] HTTP/
2090 0.002884000 54.84.148.104   192.168.1.71  HTTP     626  HTTP/1.1 200 OK  (GIF89a)
2093 0.001660000 66.165.133.65   192.168.1.71  HTTP     1201 HTTP/1.1 200 OK  (GIF89a)
2101 0.000810000 66.165.133.65   192.168.1.71  HTTP     673  HTTP/1.1 200 OK  (GIF89a)
2108 0.000778000 66.165.133.65   192.168.1.71  HTTP     324  HTTP/1.1 200 OK  (GIF89a)
2119 0.000792000 66.165.133.65   192.168.1.71  HTTP     176  HTTP/1.1 200 OK  (GIF89a)
2127 0.000527000 66.165.133.65   192.168.1.71  HTTP     591  HTTP/1.1 200 OK  (GIF89a)
2133 0.000834000 66.165.133.65   192.168.1.71  HTTP     482  HTTP/1.1 200 OK  (GIF89a)
2141 0.000479000 66.165.133.65   192.168.1.71  HTTP     592  HTTP/1.1 200 OK  (GIF89a)
2147 0.000809000 66.165.133.65   192.168.1.71  HTTP     1414 HTTP/1.1 200 OK  (GIF89a)
```

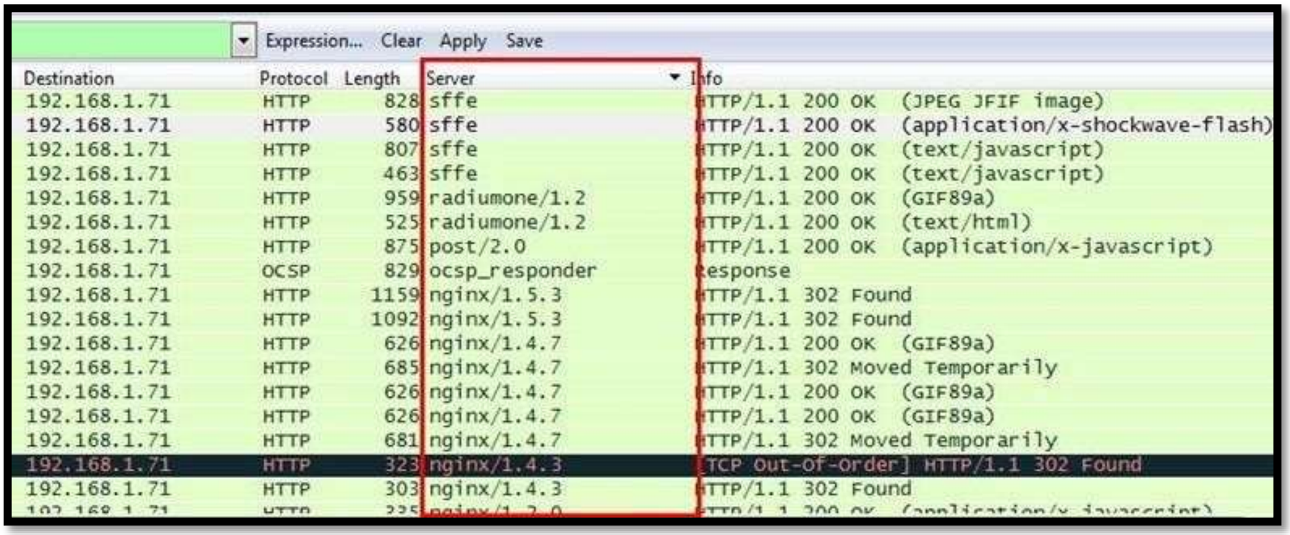
Now we will set the server header as column select any packet and right click on it then select Apply as Column.



```
Filter: http.response
No.  Time        Source
1956 0.000002000 74.12
2005 0.000745000 173.1
2023 0.038191000 209.1
2043 0.000744000 207.1
2053 0.000001000 23.21
2068 0.000745000 207.1
2084 0.006645000 209.1
2090 0.002884000 54.84
2093 0.001660000 66.16
2101 0.000810000 66.16
2108 0.000778000 66.16
2119 0.000792000 66.16
2127 0.000527000 66.16
2133 0.000834000 66.16
2141 0.000479000 66.16
2147 0.000809000 66.16
2168 0.018255000 66.16
```

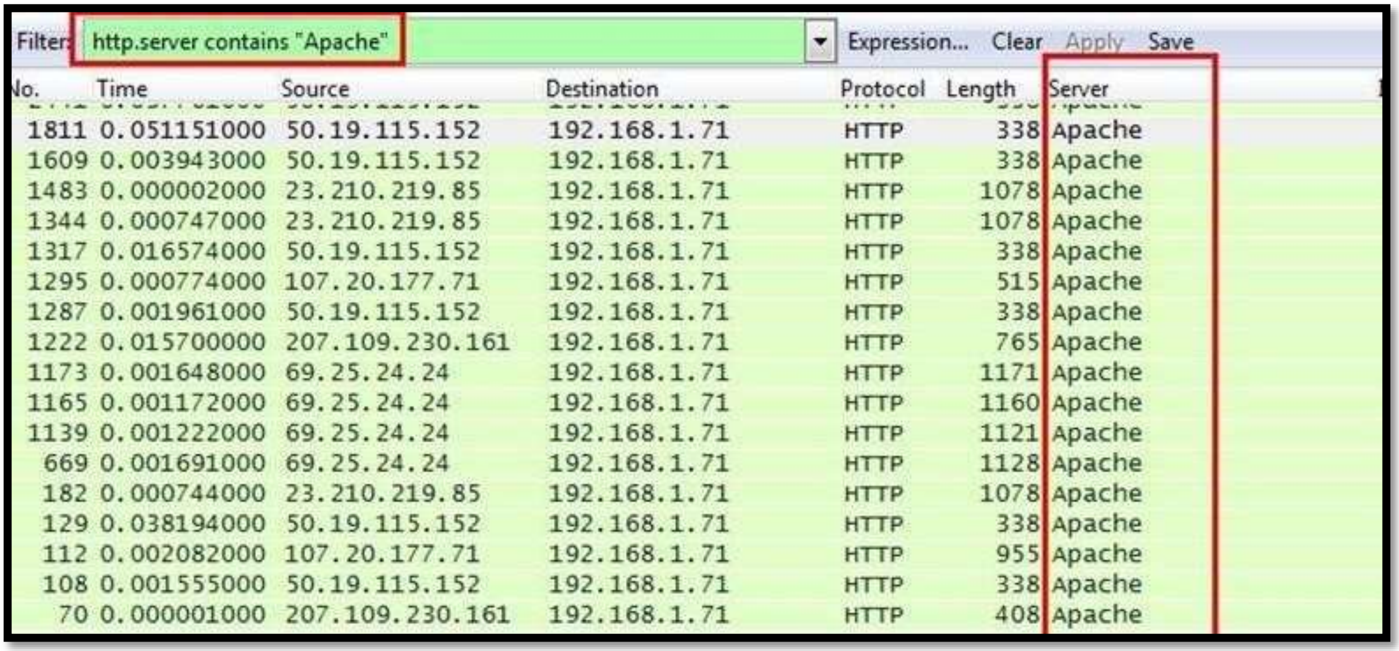
```
Date: Wed, 21 May 2
Expires: Thu, 22 Ma
Access-Control-Allo
X-Content-Type-Opti
Server: sffe\r\n
Content-Length: 40165\r\n
```

Now can see the server column where all server name is showing.



Destination	Protocol	Length	Server	Info
192.168.1.71	HTTP	828	sffe	HTTP/1.1 200 OK (JPEG JFIF image)
192.168.1.71	HTTP	580	sffe	HTTP/1.1 200 OK (application/x-shockwave-flash)
192.168.1.71	HTTP	807	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	463	sffe	HTTP/1.1 200 OK (text/javascript)
192.168.1.71	HTTP	959	radiumone/1.2	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	525	radiumone/1.2	HTTP/1.1 200 OK (text/html)
192.168.1.71	HTTP	875	post/2.0	HTTP/1.1 200 OK (application/x-javascript)
192.168.1.71	OCSP	829	ocsp_responder	Response
192.168.1.71	HTTP	1159	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	1092	nginx/1.5.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	685	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	626	nginx/1.4.7	HTTP/1.1 200 OK (GIF89a)
192.168.1.71	HTTP	681	nginx/1.4.7	HTTP/1.1 302 Moved Temporarily
192.168.1.71	HTTP	323	nginx/1.4.3	[TCP Out-Of-Order] HTTP/1.1 302 Found
192.168.1.71	HTTP	303	nginx/1.4.3	HTTP/1.1 302 Found
192.168.1.71	HTTP	335	nginx/1.2.0	HTTP/1.1 200 OK (application/x-javascript)

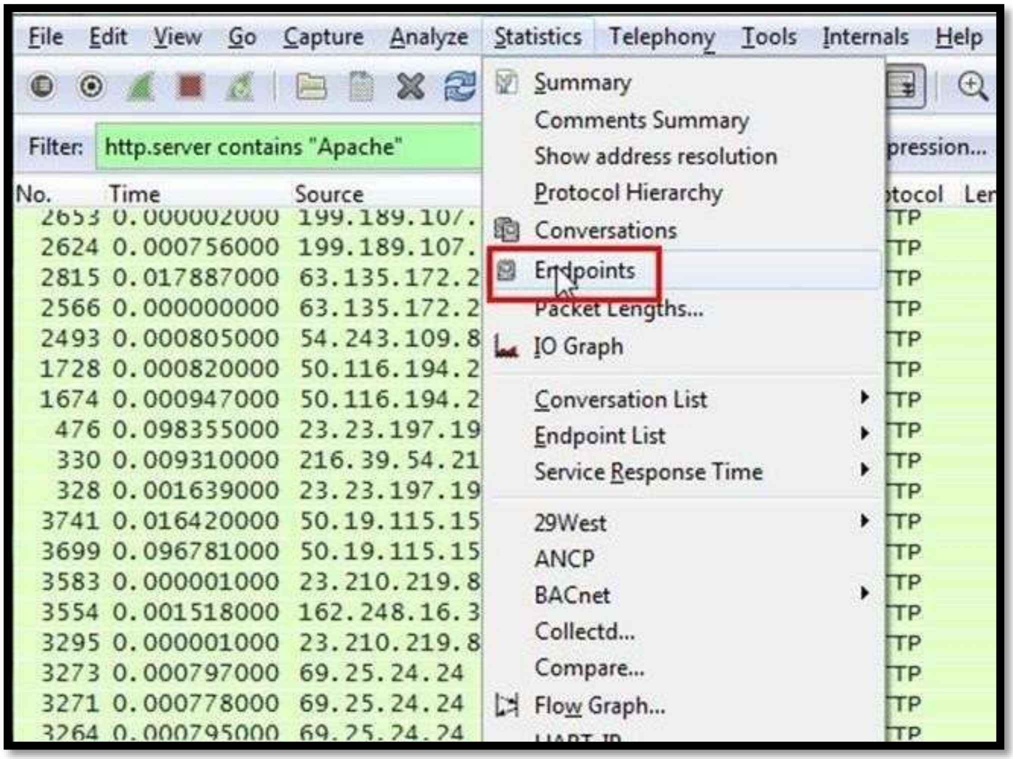
Now we have to check how many Apache packets are there we can‟t count manually for each packet so we will apply another filter http.server contains “Apache”



Filter: http.server contains "Apache"

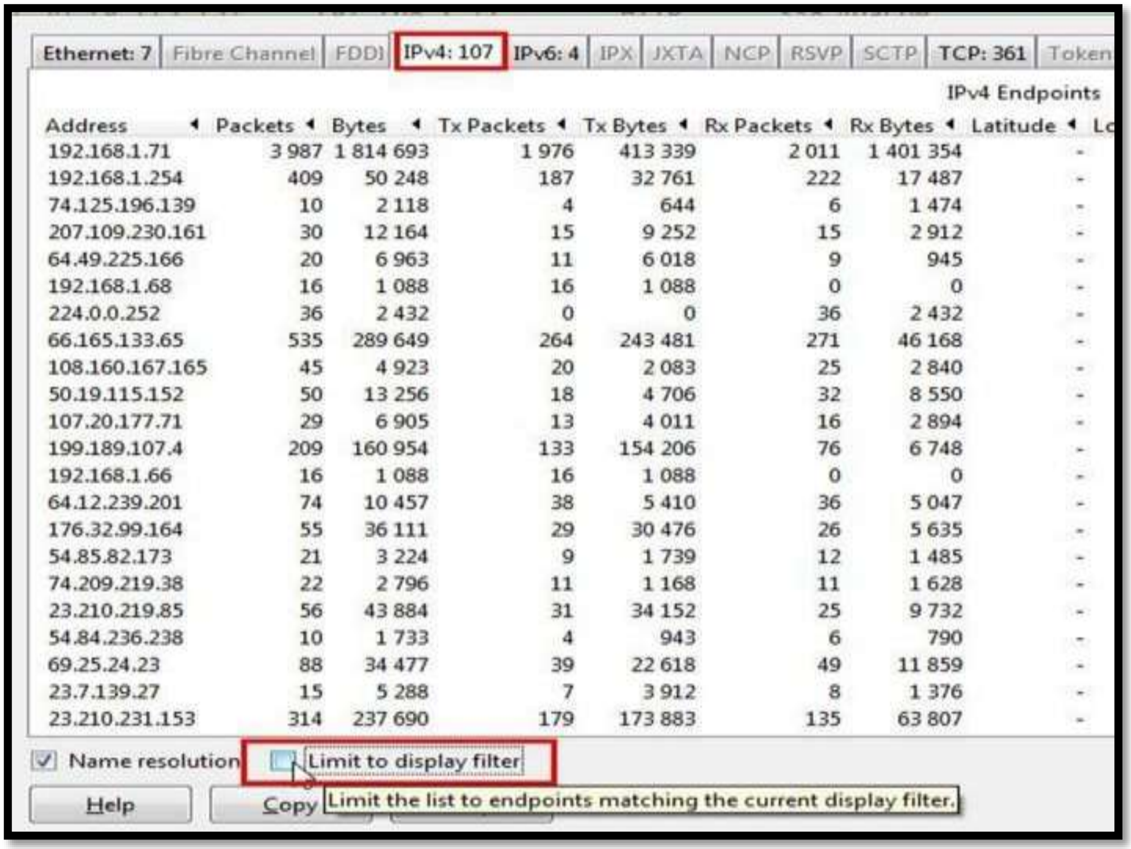
No.	Time	Source	Destination	Protocol	Length	Server
1811	0.051151000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1609	0.003943000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1483	0.000002000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1344	0.000747000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
1317	0.016574000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1295	0.000774000	107.20.177.71	192.168.1.71	HTTP	515	Apache
1287	0.001961000	50.19.115.152	192.168.1.71	HTTP	338	Apache
1222	0.015700000	207.109.230.161	192.168.1.71	HTTP	765	Apache
1173	0.001648000	69.25.24.24	192.168.1.71	HTTP	1171	Apache
1165	0.001172000	69.25.24.24	192.168.1.71	HTTP	1160	Apache
1139	0.001222000	69.25.24.24	192.168.1.71	HTTP	1121	Apache
669	0.001691000	69.25.24.24	192.168.1.71	HTTP	1128	Apache
182	0.000744000	23.210.219.85	192.168.1.71	HTTP	1078	Apache
129	0.038194000	50.19.115.152	192.168.1.71	HTTP	338	Apache
112	0.002082000	107.20.177.71	192.168.1.71	HTTP	955	Apache
108	0.001555000	50.19.115.152	192.168.1.71	HTTP	338	Apache
70	0.000001000	207.109.230.161	192.168.1.71	HTTP	408	Apache

After applying filter go to Statistics > Endpoints



Filter: http.server contains "Apache"

No.	Time	Source	tocol	Len
2653	0.000002000	199.189.107.	TP	
2624	0.000756000	199.189.107.	TP	
2815	0.017887000	63.135.172.2	TP	
2566	0.000000000	63.135.172.2	TP	
2493	0.000805000	54.243.109.8	TP	
1728	0.000820000	50.116.194.2	TP	
1674	0.000947000	50.116.194.2	TP	
476	0.098355000	23.23.197.19	TP	
330	0.009310000	216.39.54.21	TP	
328	0.001639000	23.23.197.19	TP	
3741	0.016420000	50.19.115.15	TP	
3699	0.096781000	50.19.115.15	TP	
3583	0.000001000	23.210.219.8	TP	
3554	0.001518000	162.248.16.3	TP	
3295	0.000001000	23.210.219.8	TP	
3273	0.000797000	69.25.24.24	TP	
3271	0.000778000	69.25.24.24	TP	
3264	0.000795000	69.25.24.24	TP	



IPv4 Endpoints

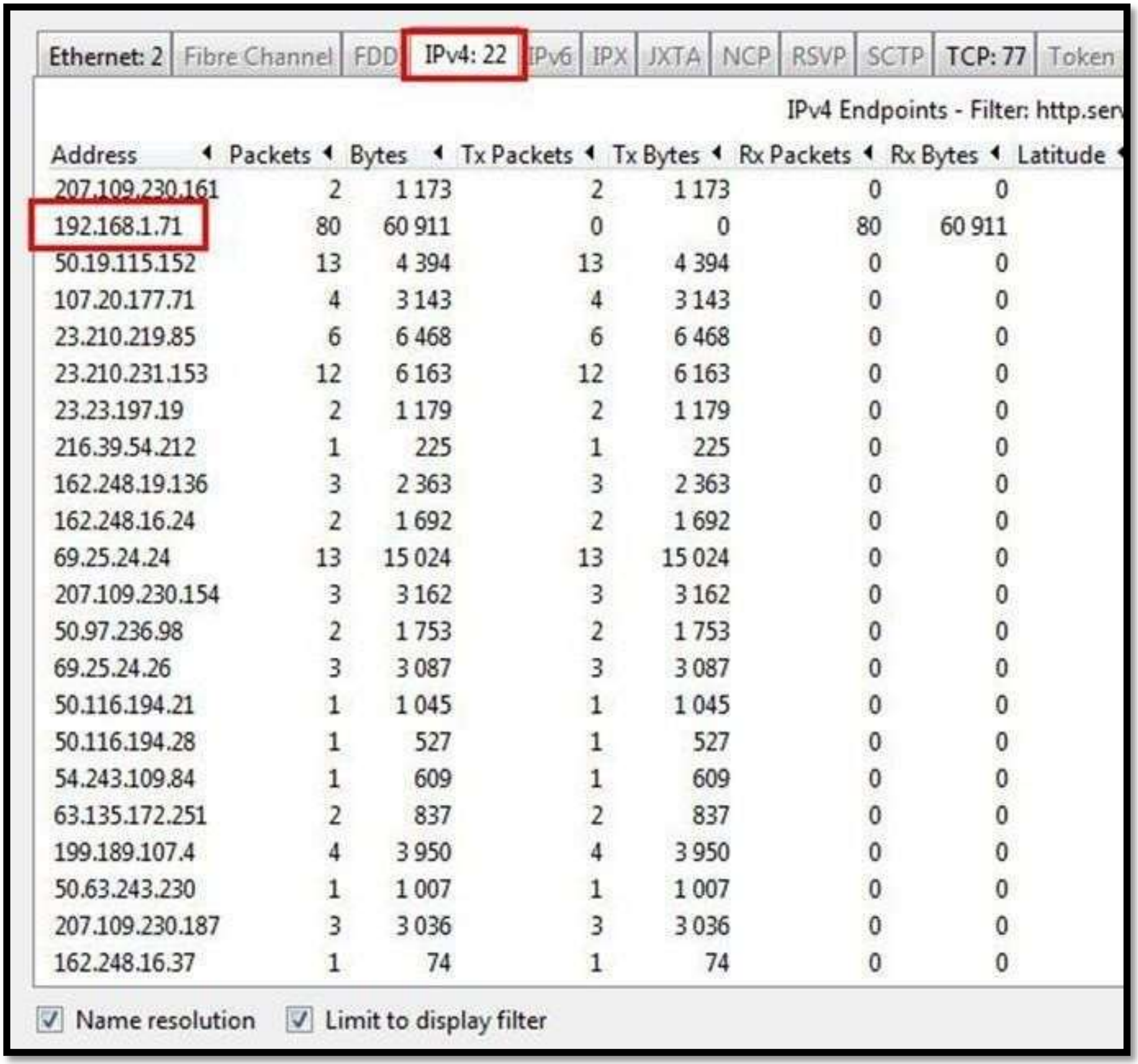
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Lo
192.168.1.71	3 987	1 814 693	1 976	413 339	2 011	1 401 354	-	
192.168.1.254	409	50 248	187	32 761	222	17 487	-	
74.125.196.139	10	2 118	4	644	6	1 474	-	
207.109.230.161	30	12 164	15	9 252	15	2 912	-	
64.49.225.166	20	6 963	11	6 018	9	945	-	
192.168.1.68	16	1 088	16	1 088	0	0	-	
224.0.0.252	36	2 432	0	0	36	2 432	-	
66.165.133.65	535	289 649	264	243 481	271	46 168	-	
108.160.167.165	45	4 923	20	2 083	25	2 840	-	
50.19.115.152	50	13 256	18	4 706	32	8 550	-	
107.20.177.71	29	6 905	13	4 011	16	2 894	-	
199.189.107.4	209	160 954	133	154 206	76	6 748	-	
192.168.1.66	16	1 088	16	1 088	0	0	-	
64.12.239.201	74	10 457	38	5 410	36	5 047	-	
176.32.99.164	55	36 111	29	30 476	26	5 635	-	
54.85.82.173	21	3 224	9	1 739	12	1 485	-	
74.209.219.38	22	2 796	11	1 168	11	1 628	-	
23.210.219.85	56	43 884	31	34 152	25	9 732	-	
54.84.236.238	10	1 733	4	943	6	790	-	
69.25.24.23	88	34 477	39	22 618	49	11 859	-	
23.7.139.27	15	5 288	7	3 912	8	1 376	-	
23.210.231.153	314	237 690	179	173 883	135	63 807	-	

☑ Name resolution □ Limit to display filter

Limit the list to endpoints matching the current display filter.

It will show all connections

Check the limit to display filter then it will show the actual Apache connections. Now there are showing 22 connections but will exclude 192.168.1.71 because it is client"s IP not a server IP so there are actual 21 Apache servers.



IPv4 Endpoints - Filter: http.ser

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude
207.109.230.161	2	1 173	2	1 173	0	0	
192.168.1.71	80	60 911	0	0	80	60 911	
50.19.115.152	13	4 394	13	4 394	0	0	
107.20.177.71	4	3 143	4	3 143	0	0	
23.210.219.85	6	6 468	6	6 468	0	0	
23.210.231.153	12	6 163	12	6 163	0	0	
23.23.197.19	2	1 179	2	1 179	0	0	
216.39.54.212	1	225	1	225	0	0	
162.248.19.136	3	2 363	3	2 363	0	0	
162.248.16.24	2	1 692	2	1 692	0	0	
69.25.24.24	13	15 024	13	15 024	0	0	
207.109.230.154	3	3 162	3	3 162	0	0	
50.97.236.98	2	1 753	2	1 753	0	0	
69.25.24.26	3	3 087	3	3 087	0	0	
50.116.194.21	1	1 045	1	1 045	0	0	
50.116.194.28	1	527	1	527	0	0	
54.243.109.84	1	609	1	609	0	0	
63.135.172.251	2	837	2	837	0	0	
199.189.107.4	4	3 950	4	3 950	0	0	
50.63.243.230	1	1 007	1	1 007	0	0	
207.109.230.187	3	3 036	3	3 036	0	0	
162.248.16.37	1	74	1	74	0	0	

☑ Name resolution ☑ Limit to display filter

CONCLUSION:- We successfully captured and analyzed network packets using Wireshark

Practical 5

Using Sysinternals tools for Network Tracking and Process Monitoring:

1. Check Sysinternals tools

=>

Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

The following are the categories of Sysinternals Tools:

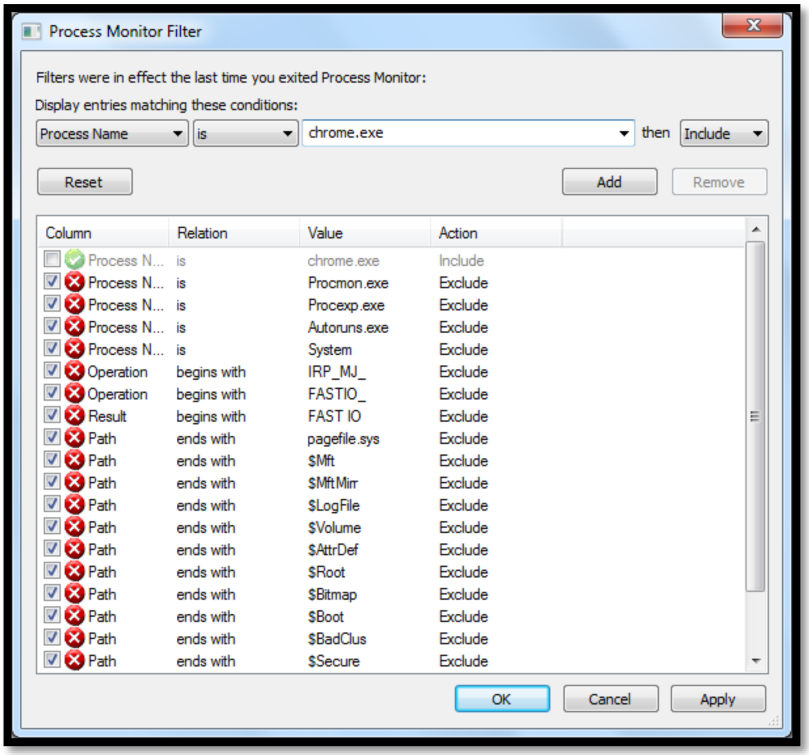
1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities

2. Monitor Live Processes (Tool: ProcMon)

=>

To Do:

1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary
4. Count Occurrences



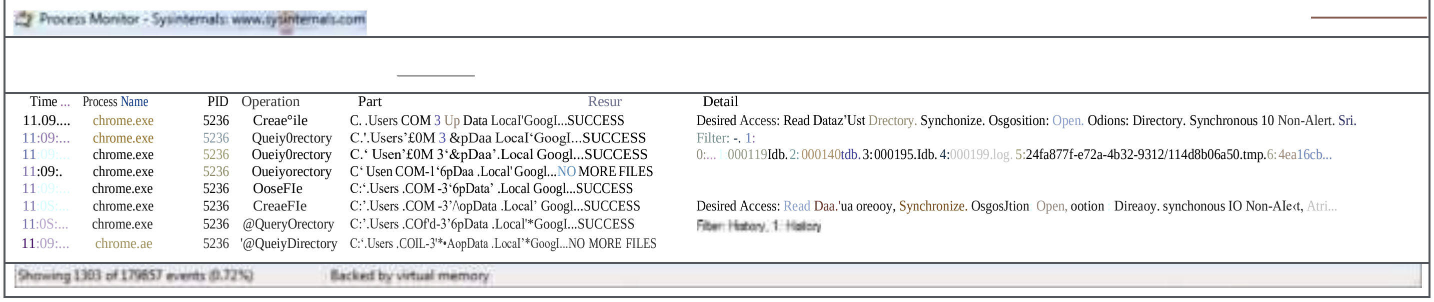
Filters were in effect the last time you exited Process Monitor:

Display entries matching these conditions:

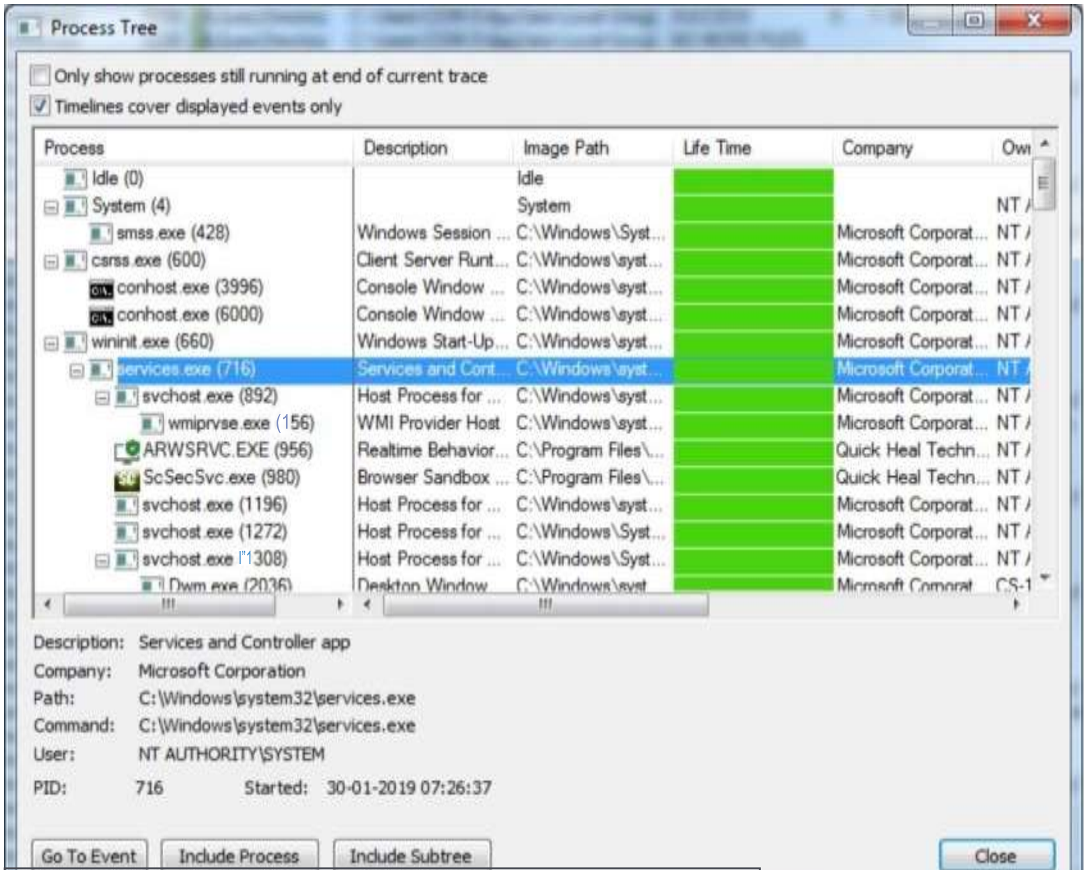
Process Name | is | chrome.exe | then | Include

Column	Relation	Value	Action
☐ ✓ Process N...	is	chrome.exe	Include
☑ ✗ Process N...	is	Procmon.exe	Exclude
☑ ✗ Process N...	is	Procexp.exe	Exclude
☑ ✗ Process N...	is	Autoruns.exe	Exclude
☑ ✗ Process N...	is	System	Exclude
☑ ✗ Operation	begins with	IRP_MJ_	Exclude
☑ ✗ Operation	begins with	FASTIO_	Exclude
☑ ✗ Result	begins with	FAST IO	Exclude
☑ ✗ Path	ends with	pagefile.sys	Exclude
☑ ✗ Path	ends with	$Mft	Exclude
☑ ✗ Path	ends with	$MftMirr	Exclude
☑ ✗ Path	ends with	$LogFile	Exclude
☑ ✗ Path	ends with	$Volume	Exclude
☑ ✗ Path	ends with	$AttrDef	Exclude
☑ ✗ Path	ends with	$Root	Exclude
☑ ✗ Path	ends with	$Bitmap	Exclude
☑ ✗ Path	ends with	$Boot	Exclude
☑ ✗ Path	ends with	$BadClus	Exclude
☑ ✗ Path	ends with	$Secure	Exclude

Output:



```
Time ...   Process Name   PID  Operation        Part                                                  Resur   Detail
11.09....  chrome.exe     5236 Creae°ile        C. .Users COM 3 Up Data Local'Googl...SUCCESS                 Desired Access: Read Dataz'Ust Drectory. Synchonize. Osgosition: Open. Odions: Directory. Synchronous 10 Non-Alert. Sri.
11:09:...  chrome.exe     5236 Queiy0rectory    C.'.Users'£0M 3 &pDaa Local'Googl...SUCCESS                   Filter: -. 1:
11:09:...  chrome.exe     5236 Oueiy0rectory    C.' Usen'£0M 3'&pDaa'.Local Googl...SUCCESS                   0:... 1:000119Idb. 2:000140tdb. 3:000195.Idb. 4:000199.log. 5:24fa877f-e72a-4b32-9312/114d8b06a50.tmp.6:4ea16cb...
11:09:.    chrome.exe     5236 Oueiyorectory    C' Usen COM-1'6pDaa .Local' Googl...NO MORE FILES
11:09:...  chrome.exe     5236 OoseFIe          C:'.Users .COM -3'6pData' .Local Googl...SUCCESS
11:0S:...  chrome.exe     5236 CreaeFIe         C:'.Users .COM -3'/\opData .Local' Googl...SUCCESS            Desired Access: Read Daa.'ua oreooy, Synchronize. OsgosJtion Open, ootion Direaoy. synchonous IO Non-AIe‹t, Atri...
11:0S:...  chrome.exe     5236 @QueryOrectory   C:'.Users .COf'd-3'6pData .Local'*Googl...SUCCESS             Fiber: History, 1: History
11:09:...  chrome.ae      5236 '@QueiyDirectory C:'.Users .COIL-3'*•AopData .Local'*Googl...NO MORE FILES
Showing 1303 of 179857 events (0.72%)          Backed by virtual memory
```



□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Own
Idle (0)		Idle	🟩		
System (4)		System	🟩		NT /
smss.exe (428)	Windows Session ...	C:\Windows\Syst...	🟩	Microsoft Corporat...	NT /
csrss.exe (600)	Client Server Runt...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
conhost.exe (3996)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
conhost.exe (6000)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
wininit.exe (660)	Windows Start-Up...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
services.exe (716)	Services and Cont...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
svchost.exe (892)	Host Process for ...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
wmiprvse.exe (156)	WMI Provider Host	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
ARWSRVC.EXE (956)	Realtime Behavior...	C:\Program Files\...	🟩	Quick Heal Techn...	NT /
ScSecSvc.exe (980)	Browser Sandbox ...	C:\Program Files\...	🟩	Quick Heal Techn...	NT /
svchost.exe (1196)	Host Process for ...	C:\Windows\syst...	🟩	Microsoft Corporat...	NT /
svchost.exe (1272)	Host Process for ...	C:\Windows\Syst...	🟩	Microsoft Corporat...	NT /
svchost.exe l"1308)	Host Process for ...	C:\Windows\Syst...	🟩	Microsoft Corporat...	NT /
Dwm.exe (2036)	Desktop Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	CS-1

Description: Services and Controller app

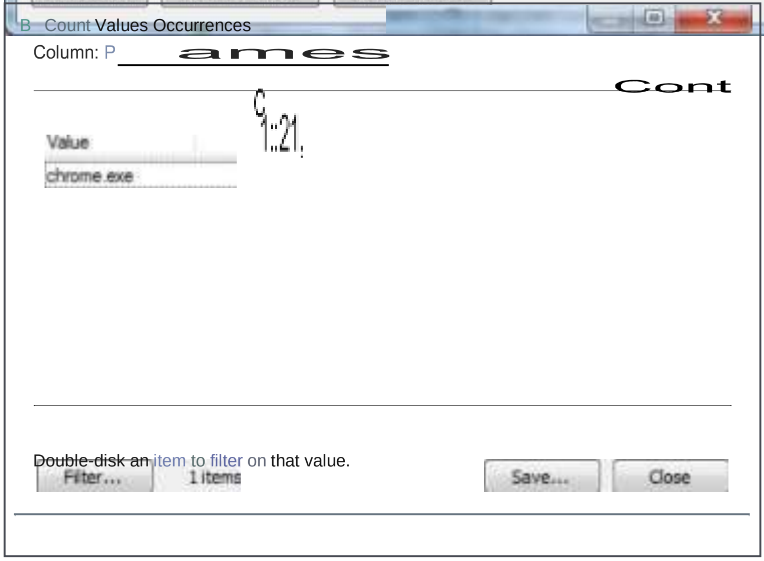
Company: Microsoft Corporation

Path: C:\Windows\system32\services.exe

Command: C:\Windows\system32\services.exe

User: NT AUTHORITY\SYSTEM

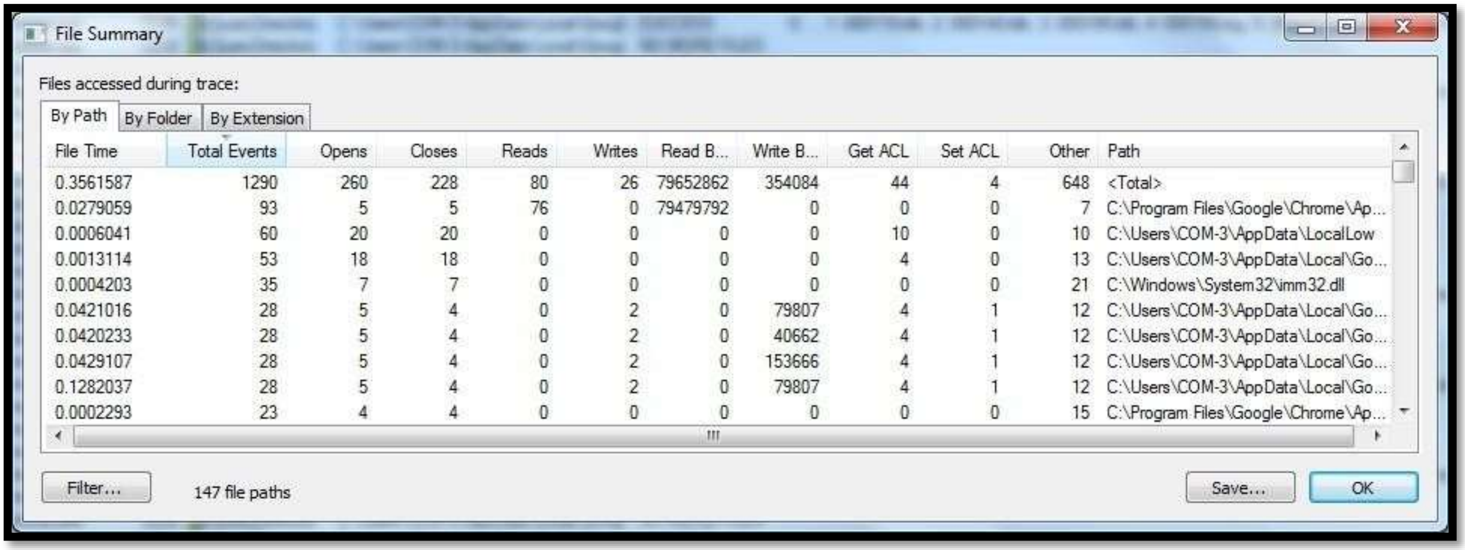
PID: 716 Started: 30-01-2019 07:26:37



Column: P ames

Value	Cont
chrome.exe	1:21

Double-disk an item to filter on that value.



Files accessed during trace:

File Time	Total Events	Opens	Closes	Reads	Writes	Read B...	Write B...	Get ACL	Set ACL	Other	Path
0.3561587	1290	260	228	80	26	79652862	354084	44	4	648	<Total>
0.0279059	93	5	5	76	0	79479792	0	0	0	7	C:\Program Files\Google\Chrome\Ap...
0.0006041	60	20	20	0	0	0	0	10	0	10	C:\Users\COM-3\AppData\LocalLow
0.0013114	53	18	18	0	0	0	0	4	0	13	C:\Users\COM-3\AppData\Local\Go...
0.0004203	35	7	7	0	0	0	0	0	0	21	C:\Windows\System32\imm32.dll
0.0421016	28	5	4	0	2	0	79807	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0420233	28	5	4	0	2	0	40662	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0429107	28	5	4	0	2	0	153666	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.1282037	28	5	4	0	2	0	79807	4	1	12	C:\Users\COM-3\AppData\Local\Go...
0.0002293	23	4	4	0	0	0	0	0	0	15	C:\Program Files\Google\Chrome\Ap...

147 file paths

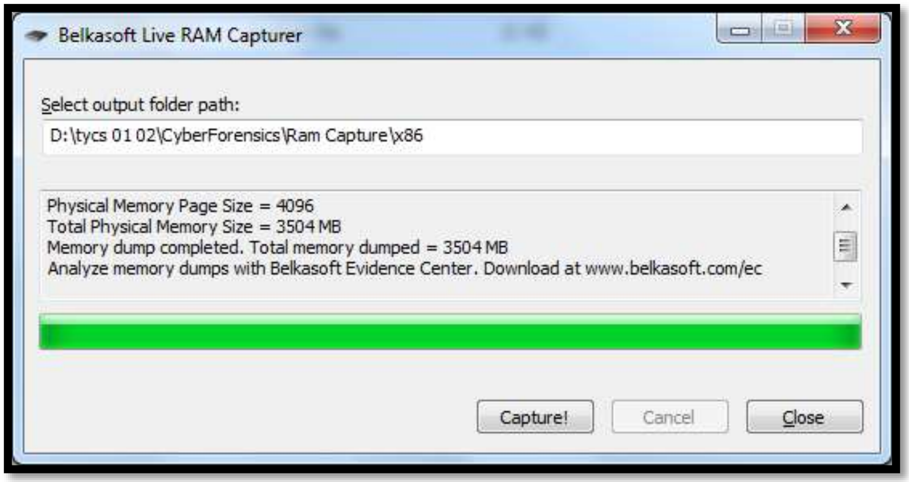
3. Capture RAM (Tool: RAMCapture)

=>

To Do:

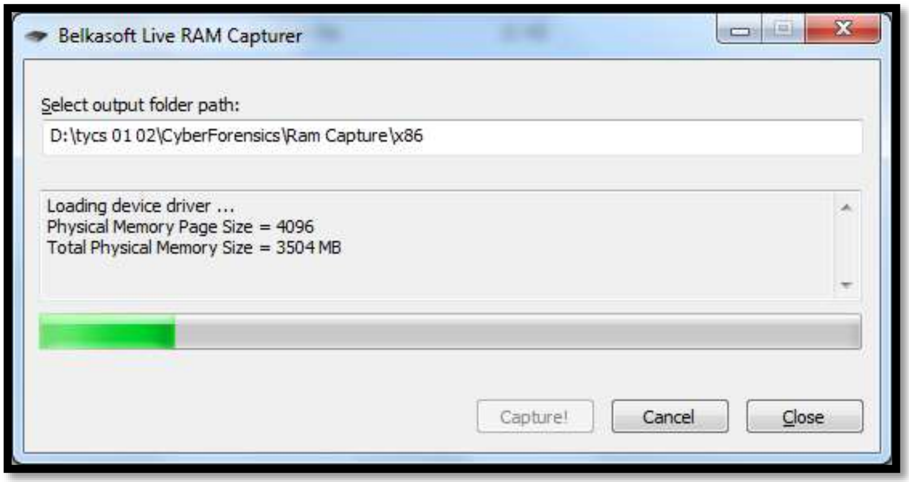
1. Click Capture
2. Creates a .mem file of the system memory (RAM) utilized.

Output:



Select output folder path: D:\tycs 01 02\CyberForensics\Ram Capture\x86

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 3504 MB
Memory dump completed. Total memory dumped = 3504 MB
Analyze memory dumps with Belkasoft Evidence Center. Download at www.belkasoft.com/ec
```



Select output folder path:

D:\tycs 01 02\CyberForensics\Ram Capture\x86

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 3504 MB
```

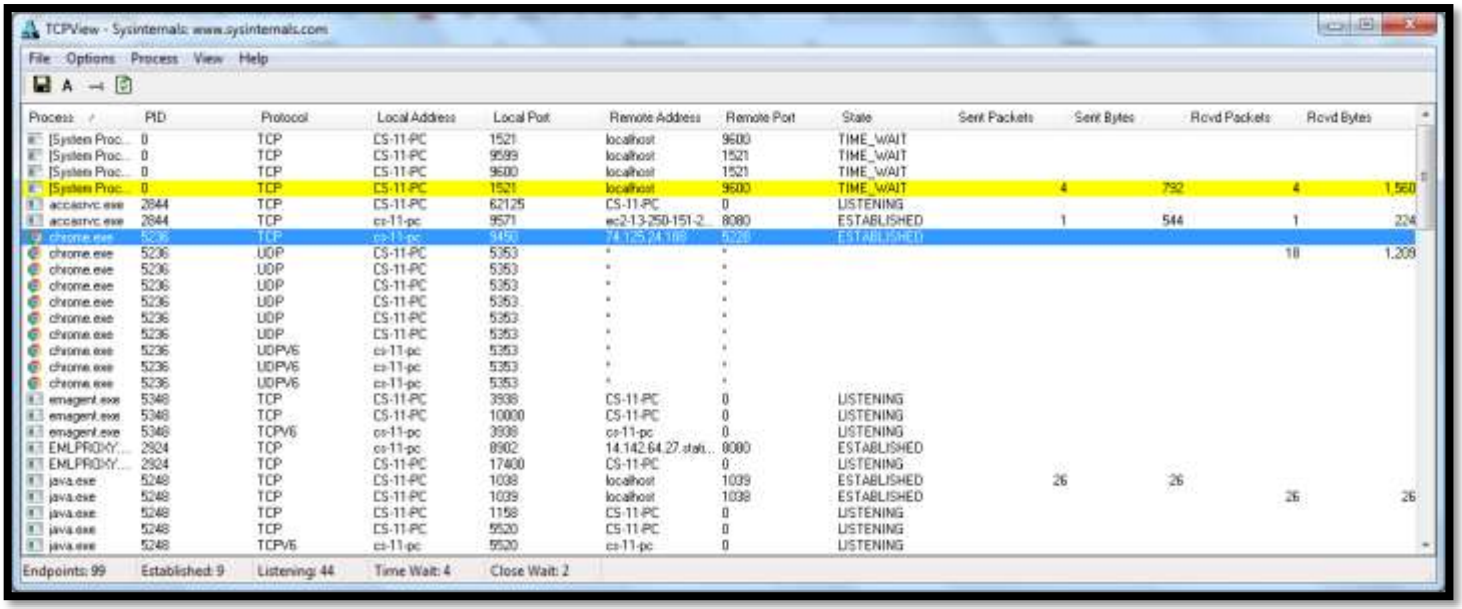
4. Capture TCP/UDP packets (Tool: TcpView)

=>

To Do:

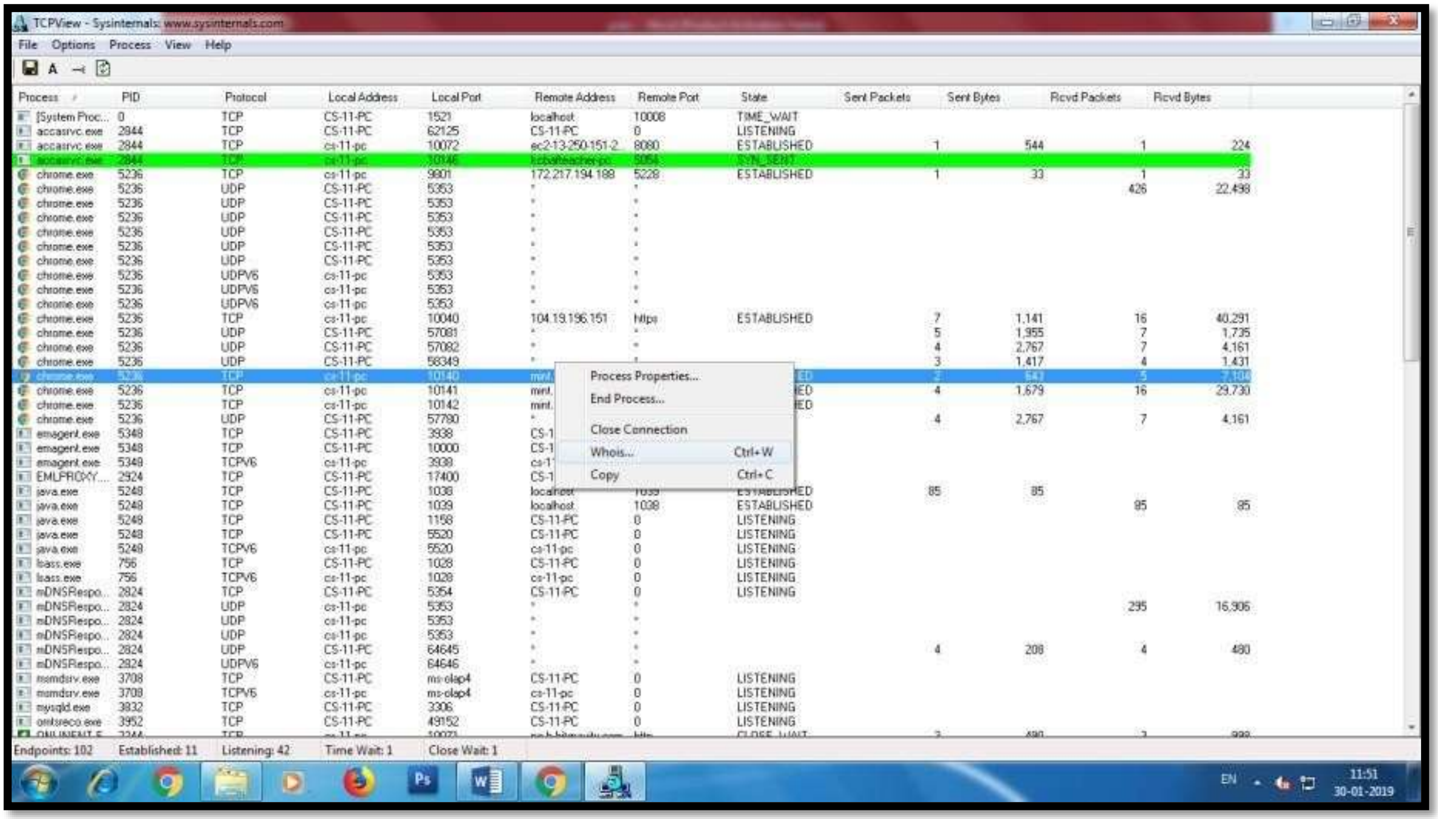
1. Save to .txt file.
2. Whois

Output:



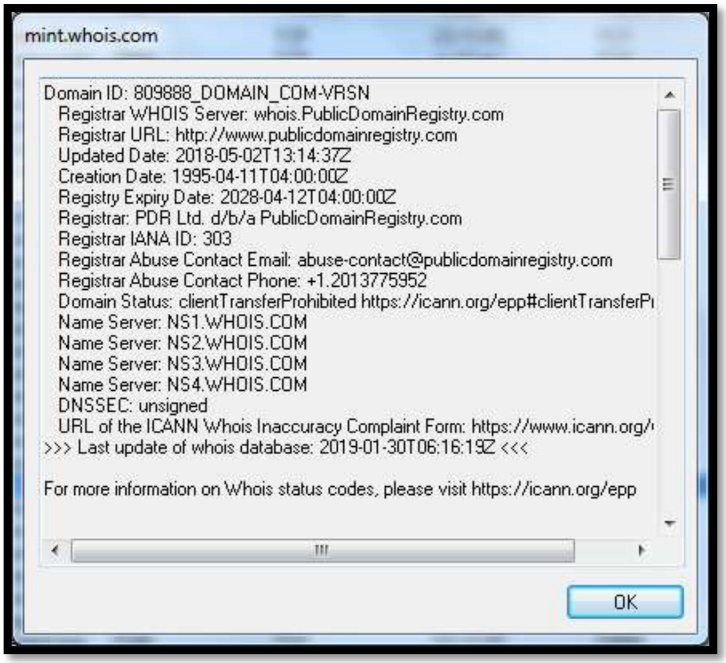
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT				
[System Proc...	0	TCP	CS-11-PC	9599	localhost	1521	TIME_WAIT				
[System Proc...	0	TCP	CS-11-PC	9600	localhost	1521	TIME_WAIT				
[System Proc...	0	TCP	CS-11-PC	1521	localhost	9600	TIME_WAIT	4	792	4	1,560
accasrvc.exe	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accasrvc.exe	2844	TCP	cs-11-pc	9571	ec2-13-250-151-2...	8080	ESTABLISHED	1	544	1	224
chrome.exe	5236	TCP	cs-11-pc	9450	74.125.24.188	5228	ESTABLISHED				
chrome.exe	5236	UDP	CS-11-PC	5353	*	*				18	1,209
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
emagent.exe	5348	TCP	CS-11-PC	3938	CS-11-PC	0	LISTENING				
emagent.exe	5348	TCP	CS-11-PC	10000	CS-11-PC	0	LISTENING				
emagent.exe	5348	TCPV6	cs-11-pc	3938	cs-11-pc	0	LISTENING				
EMLPROXY....	2924	TCP	cs-11-pc	8902	14.142.64.27.stati...	8080	ESTABLISHED				
EMLPROXY....	2924	TCP	CS-11-PC	17400	CS-11-PC	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	1038	localhost	1039	ESTABLISHED	26	26		
java.exe	5248	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED			26	26
java.exe	5248	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe	5248	TCPV6	cs-11-pc	5520	cs-11-pc	0	LISTENING				

Endpoints: 99 Established: 9 Listening: 44 Time Wait: 4 Close Wait: 2



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	CS-11-PC	1521	localhost	10008	TIME_WAIT				
accasrvc.exe	2844	TCP	CS-11-PC	62125	CS-11-PC	0	LISTENING				
accasrvc.exe	2844	TCP	cs-11-pc	10072	ec2-13-250-151-2...	8080	ESTABLISHED	1	544	1	224
accasrvc.exe	2844	TCP	cs-11-pc	10146	kcbalteacher-pc	5054	SYN_SENT				
chrome.exe	5236	TCP	cs-11-pc	9801	172.217.194.188	5228	ESTABLISHED	1	33	1	33
chrome.exe	5236	UDP	CS-11-PC	5353	*	*				426	22,498
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDP	CS-11-PC	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	UDPV6	cs-11-pc	5353	*	*					
chrome.exe	5236	TCP	cs-11-pc	10040	104.19.196.151	https	ESTABLISHED	7	1,141	16	40,291
chrome.exe	5236	UDP	CS-11-PC	57081	*	*		5	1,955	7	1,735
chrome.exe	5236	UDP	CS-11-PC	57082	*	*		4	2,767	7	4,161
chrome.exe	5236	UDP	CS-11-PC	58349	*	*		3	1,417	4	1,431
chrome.exe	5236	TCP	cs-11-pc	10140	mint.		ED	2	643	5	7,104
chrome.exe	5236	TCP	cs-11-pc	10141	mint.		IED	4	1,679	16	29,730
chrome.exe	5236	TCP	cs-11-pc	10142	mint.		IED				
chrome.exe	5236	UDP	CS-11-PC	57780	*			4	2,767	7	4,161
emagent.exe	5348	TCP	CS-11-PC	3938	CS-1						
emagent.exe	5348	TCP	CS-11-PC	10000	CS-1						
emagent.exe	5348	TCPV6	cs-11-pc	3938	cs-1						
EMLPROXY....	2924	TCP	CS-11-PC	17400	CS-1						
java.exe	5248	TCP	CS-11-PC	1038	localhost	1039	ESTABLISHED	85	85		
java.exe	5248	TCP	CS-11-PC	1039	localhost	1038	ESTABLISHED			85	85
java.exe	5248	TCP	CS-11-PC	1158	CS-11-PC	0	LISTENING				
java.exe	5248	TCP	CS-11-PC	5520	CS-11-PC	0	LISTENING				
java.exe	5248	TCPV6	cs-11-pc	5520	cs-11-pc	0	LISTENING				
lsass.exe	756	TCP	CS-11-PC	1028	CS-11-PC	0	LISTENING				
lsass.exe	756	TCPV6	cs-11-pc	1028	cs-11-pc	0	LISTENING				
mDNSRespo...	2824	TCP	CS-11-PC	5354	CS-11-PC	0	LISTENING				
mDNSRespo...	2824	UDP	cs-11-pc	5353	*	*				295	16,906
mDNSRespo...	2824	UDP	cs-11-pc	5353	*	*					
mDNSRespo...	2824	UDP	cs-11-pc	5353	*	*					
mDNSRespo...	2824	UDP	CS-11-PC	64645	*	*		4	208	4	480
mDNSRespo...	2824	UDPV6	cs-11-pc	64646	*	*					
msmdsrv.exe	3708	TCP	CS-11-PC	ms-olap4	CS-11-PC	0	LISTENING				
msmdsrv.exe	3708	TCPV6	cs-11-pc	ms-olap4	cs-11-pc	0	LISTENING				
mysqld.exe	3832	TCP	CS-11-PC	3306	CS-11-PC	0	LISTENING				
omtsreco.exe	3952	TCP	CS-11-PC	49152	CS-11-PC	0	LISTENING				
ONLINENT.E...	2244	TCP	cs-11-pc	10071	[illegible]	http	CLOSE_WAIT	3	480	3	999

Endpoints: 102 Established: 11 Listening: 42 Time Wait: 1 Close Wait: 1



```
Domain ID: 809888_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.PublicDomainRegistry.com
   Registrar URL: http://www.publicdomainregistry.com
   Updated Date: 2018-05-02T13:14:37Z
   Creation Date: 1995-04-11T04:00:00Z
   Registry Expiry Date: 2028-04-12T04:00:00Z
   Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
   Registrar IANA ID: 303
   Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
   Registrar Abuse Contact Phone: +1.2013775952
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPı
   Name Server: NS1.WHOIS.COM
   Name Server: NS2.WHOIS.COM
   Name Server: NS3.WHOIS.COM
   Name Server: NS4.WHOIS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/
>>> Last update of whois database: 2019-01-30T06:16:19Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

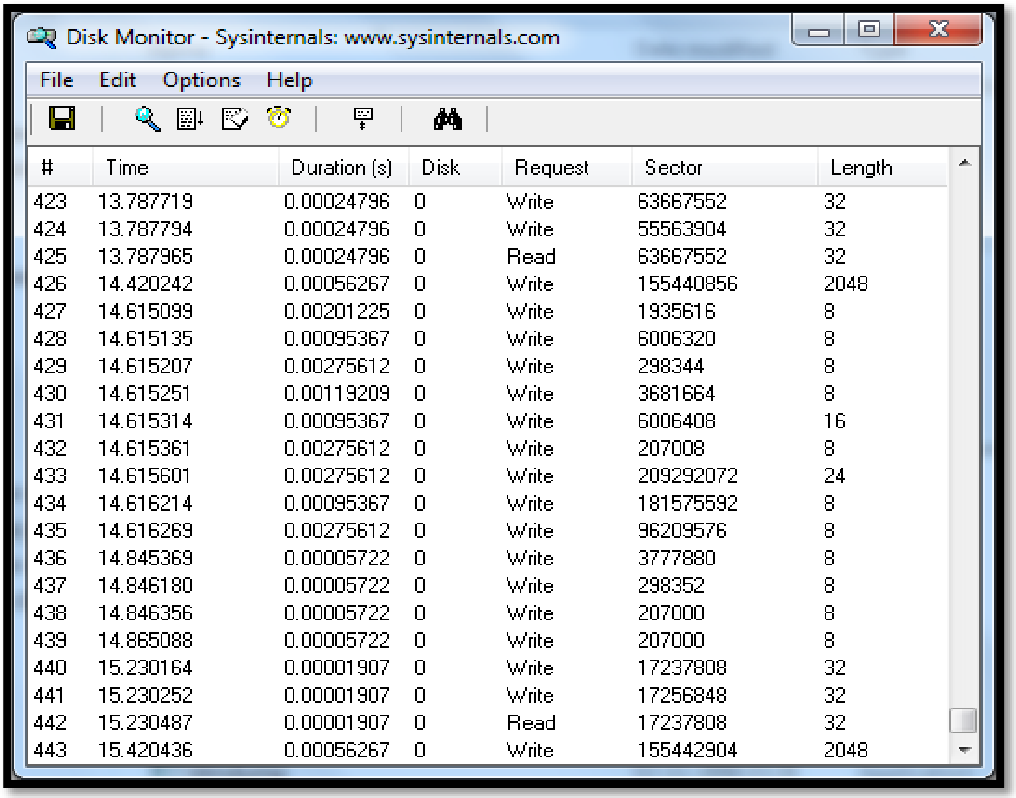
5. Monitor Hard Disk (Tool: DiskMon)

=>

To Do:

1. Save to .log file.
2. Check operations performed in the disk as per time and sectors affected.

Output:



#	Time	Duration (s)	Disk	Request	Sector	Length
423	13.787719	0.00024796	0	Write	63667552	32
424	13.787794	0.00024796	0	Write	55563904	32
425	13.787965	0.00024796	0	Read	63667552	32
426	14.420242	0.00056267	0	Write	155440856	2048
427	14.615099	0.00201225	0	Write	1935616	8
428	14.615135	0.00095367	0	Write	6006320	8
429	14.615207	0.00275612	0	Write	298344	8
430	14.615251	0.00119209	0	Write	3681664	8
431	14.615314	0.00095367	0	Write	6006408	16
432	14.615361	0.00275612	0	Write	207008	8
433	14.615601	0.00275612	0	Write	209292072	24
434	14.616214	0.00095367	0	Write	181575592	8
435	14.616269	0.00275612	0	Write	96209576	8
436	14.845369	0.00005722	0	Write	3777880	8
437	14.846180	0.00005722	0	Write	298352	8
438	14.846356	0.00005722	0	Write	207000	8
439	14.865088	0.00005722	0	Write	207000	8
440	15.230164	0.00001907	0	Write	17237808	32
441	15.230252	0.00001907	0	Write	17256848	32
442	15.230487	0.00001907	0	Read	17237808	32
443	15.420436	0.00056267	0	Write	155442904	2048

6. Monitor Virtual Memory (Tool: VMMap)

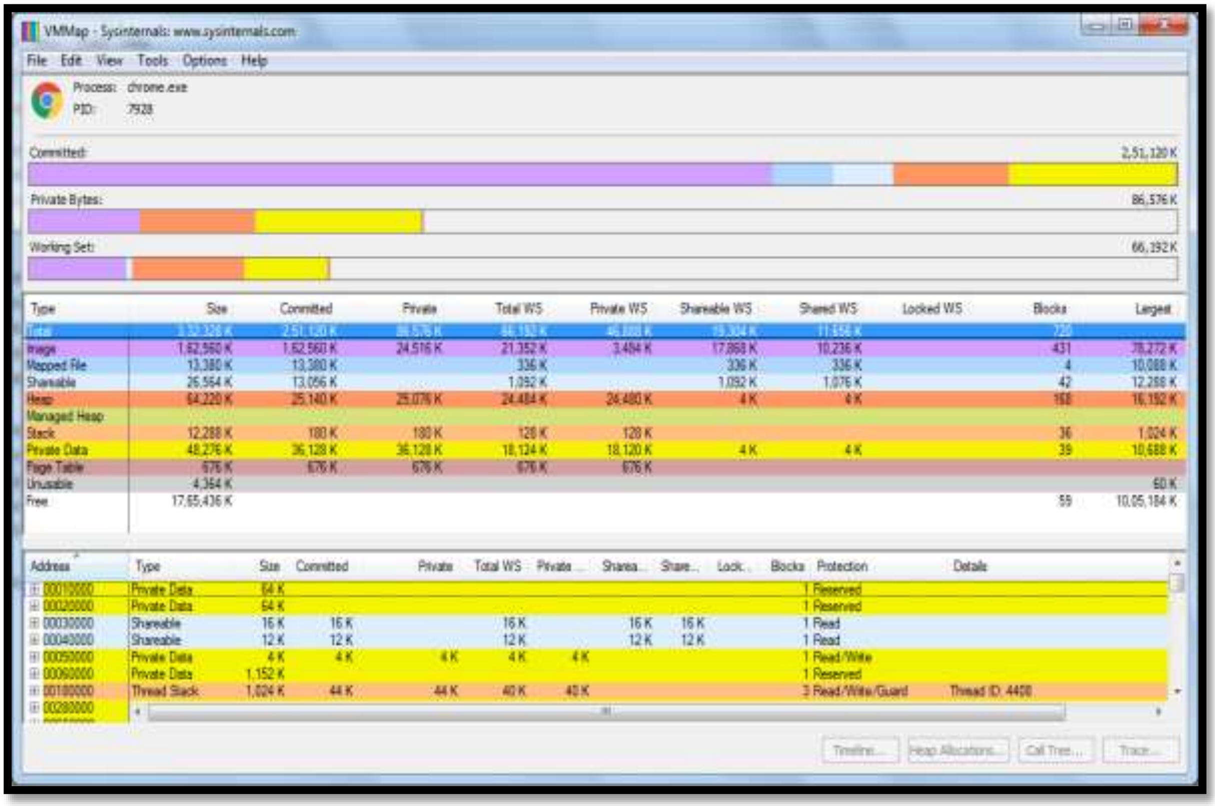
=>

To Do:

1. Options – Show Free & Unusable Regions

2. File-> Select Process e.g. chrome.exe
3. Save to .mmp file.

Output:



Process: chrome.exe

PID: 7928

Committed: 2,51,120 K

Private Bytes: 86,576 K

Working Set: 66,192 K

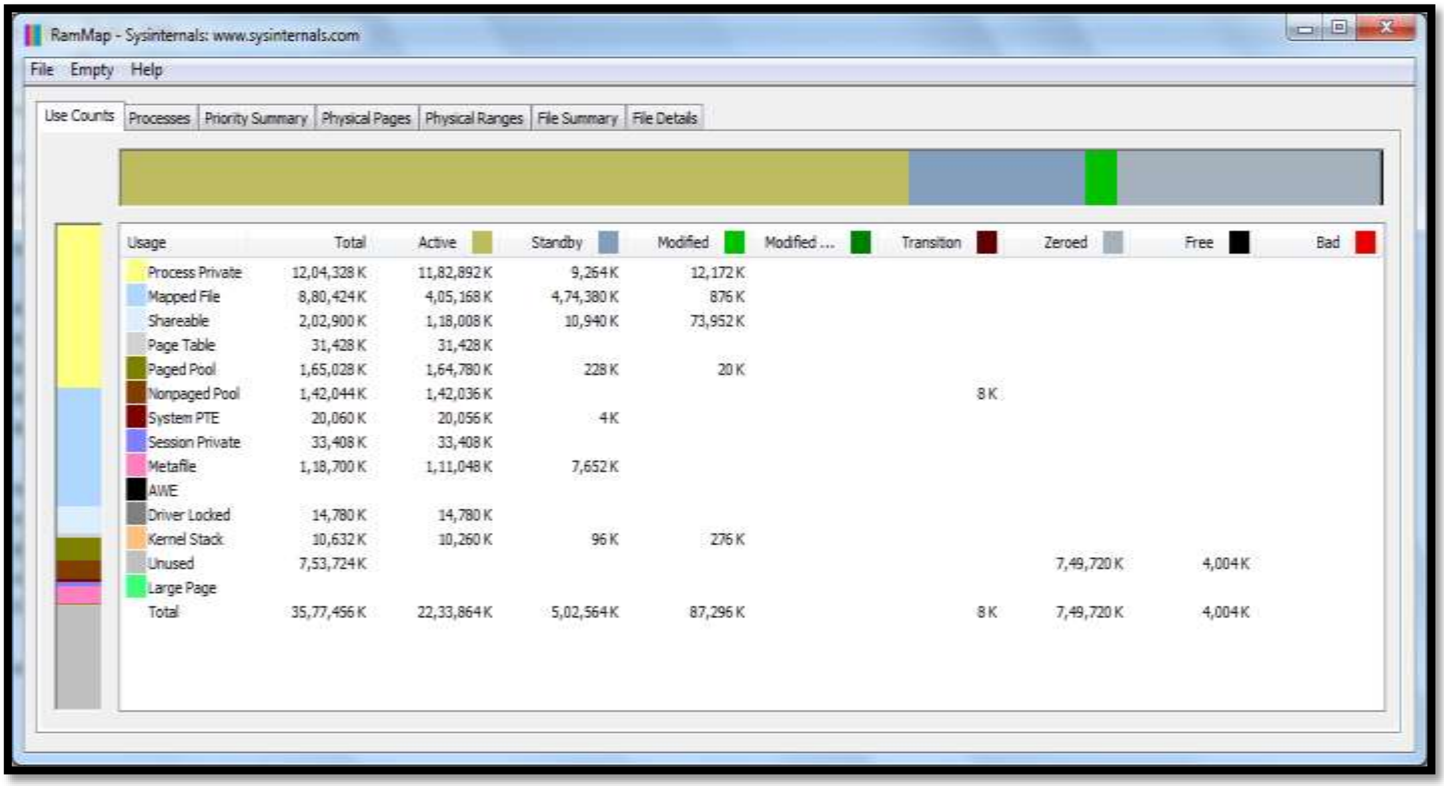
Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Locked WS	Blocks	Largest
Total	3,32,328 K	2,51,120 K	86,576 K	66,192 K	46,888 K	19,304 K	11,656 K		720	
Image	1,62,560 K	1,62,560 K	24,516 K	21,352 K	3,484 K	17,868 K	10,236 K		431	78,272 K
Mapped File	13,380 K	13,380 K		336 K		336 K	336 K		4	10,088 K
Shareable	26,564 K	13,056 K		1,092 K		1,092 K	1,076 K		42	12,288 K
Heap	64,220 K	25,140 K	25,076 K	24,484 K	24,480 K	4 K	4 K		168	16,192 K
Managed Heap										
Stack	12,288 K	180 K	180 K	128 K	128 K				36	1,024 K
Private Data	48,276 K	36,128 K	36,128 K	18,124 K	18,120 K	4 K	4 K		39	10,688 K
Page Table	676 K	676 K	676 K	676 K	676 K					
Unusable	4,364 K									60 K
Free	17,65,436 K								59	10,05,184 K

Address	Type	Size	Committed	Private	Total WS	Private ...	Sharea...	Share...	Lock...	Blocks	Protection	Details
⊞ 00010000	Private Data	64 K								1	Reserved	
⊞ 00020000	Private Data	64 K								1	Reserved	
⊞ 00030000	Shareable	16 K	16 K		16 K		16 K	16 K		1	Read	
⊞ 00040000	Shareable	12 K	12 K		12 K		12 K	12 K		1	Read	
⊞ 00050000	Private Data	4 K	4 K	4 K	4 K	4 K				1	Read/Write	
⊞ 00060000	Private Data	1,152 K								1	Reserved	
⊞ 00180000	Thread Stack	1,024 K	44 K	44 K	40 K	40 K				3	Read/Write/Guard	Thread ID: 4408
⊞ 00280000												

7. Monitor Cache Memory (Tool: RAMMap)To Do:

1. Save to .RMP file.

Output:



Usage	Total	Active 🟨	Standby 🟦	Modified 🟩	Modified ... 🟩	Transition 🟫	Zeroed ⬜	Free ⬛	Bad 🟥
🟨 Process Private	12,04,328 K	11,82,892 K	9,264 K	12,172 K					
🟦 Mapped File	8,80,424 K	4,05,168 K	4,74,380 K	876 K					
⬜ Shareable	2,02,900 K	1,18,008 K	10,940 K	73,952 K					
⬜ Page Table	31,428 K	31,428 K							
🟫 Paged Pool	1,65,028 K	1,64,780 K	228 K	20 K					
🟫 Nonpaged Pool	1,42,044 K	1,42,036 K				8 K			
🟥 System PTE	20,060 K	20,056 K	4 K						
🟪 Session Private	33,408 K	33,408 K							
🟪 Metafile	1,18,700 K	1,11,048 K	7,652 K						
⬛ AWE									
⬛ Driver Locked	14,780 K	14,780 K							
🟧 Kernel Stack	10,632 K	10,260 K	96 K	276 K					
⬜ Unused	7,53,724 K						7,49,720 K	4,004 K	
🟩 Large Page									
Total	35,77,456 K	22,33,864 K	5,02,564 K	87,296 K		8 K	7,49,720 K	4,004 K	

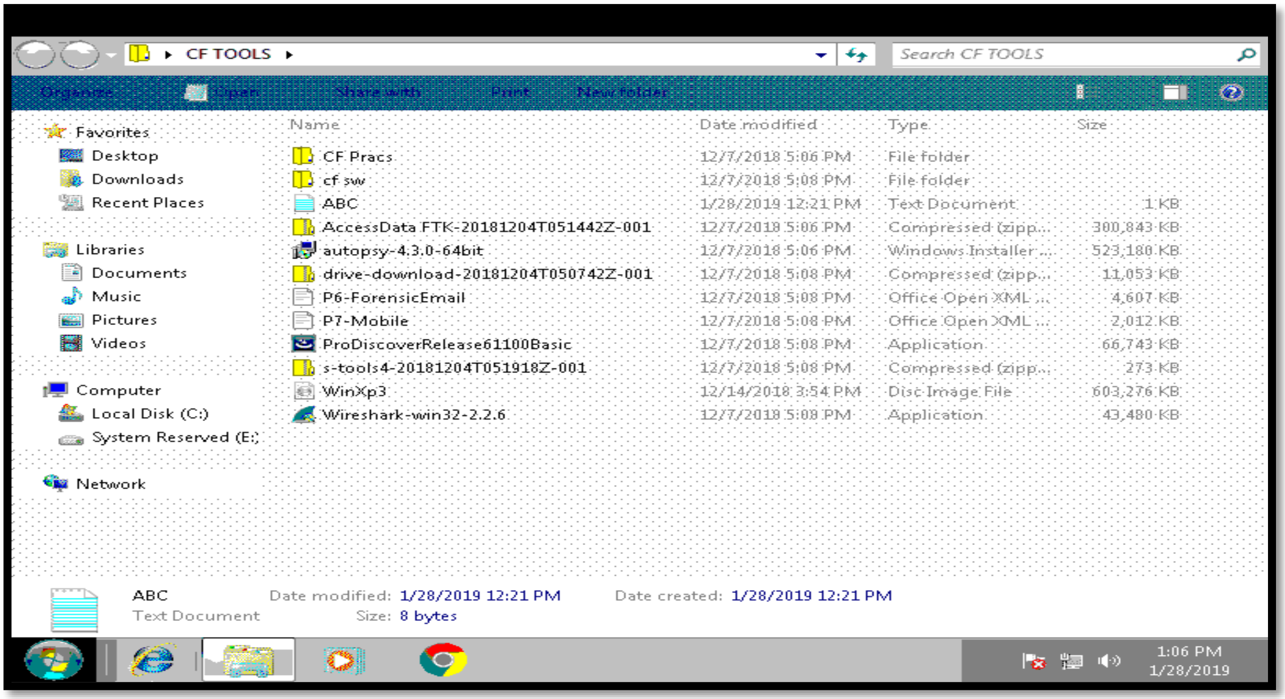
CONCLUSION:- We successfully used Sysinternals tools for Network Tracking and Process Monitoring

Practical 6

Aim :- Recovering And Inspecting Deleted Files Using Access Data FTK.

Step 1:-

Create any demo text file and save it .

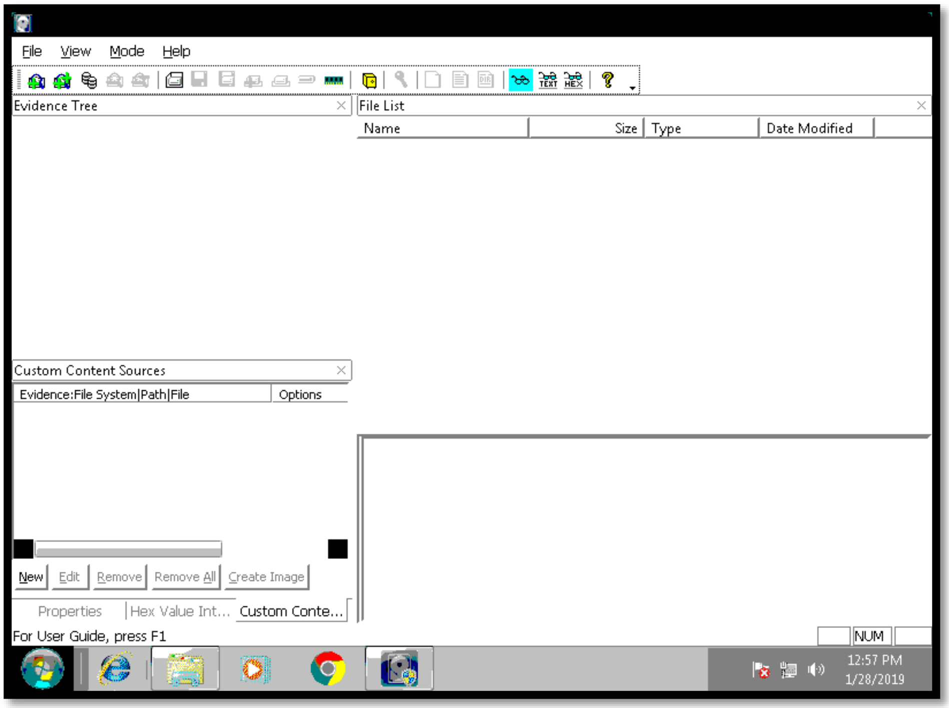


Name	Date modified	Type	Size
CF Pracs	12/7/2018 5:06 PM	File folder	
cf sw	12/7/2018 5:08 PM	File folder	
ABC	1/28/2019 12:21 PM	Text Document	1 KB
AccessData FTK-20181204T051442Z-001	12/7/2018 5:06 PM	Compressed (zipp...	300,843 KB
autopsy-4.3.0-64bit	12/7/2018 5:06 PM	Windows Installer ...	523,180 KB
drive-download-20181204T050742Z-001	12/7/2018 5:08 PM	Compressed (zipp...	11,053 KB
P6-ForensicEmail	12/7/2018 5:08 PM	Office Open XML ...	4,607 KB
P7-Mobile	12/7/2018 5:08 PM	Office Open XML ...	2,012 KB
ProDiscoverRelease61100Basic	12/7/2018 5:08 PM	Application	66,743 KB
s-tools4-20181204T051918Z-001	12/7/2018 5:08 PM	Compressed (zipp...	273 KB
WinXp3	12/14/2018 3:54 PM	Disc Image File	603,276 KB
Wireshark-win32-2.2.6	12/7/2018 5:08 PM	Application	43,480 KB

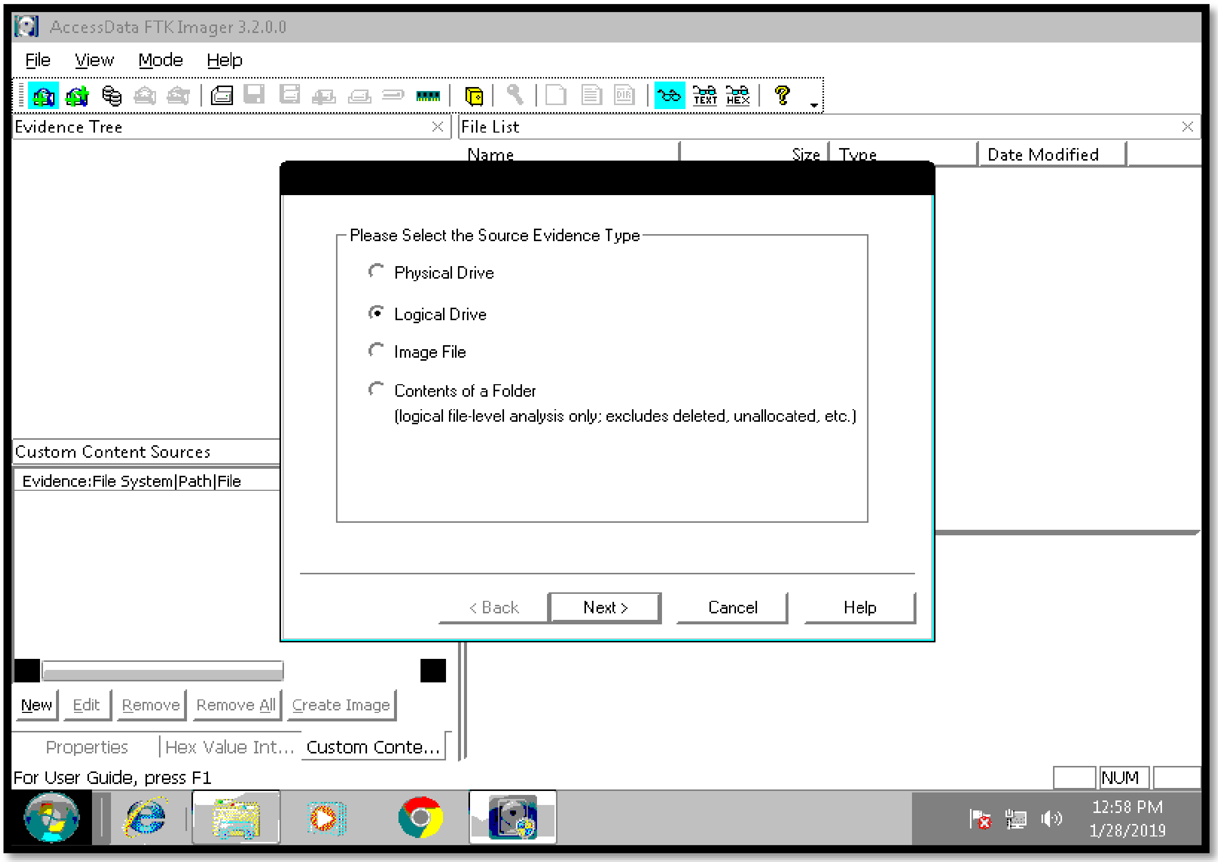
ABC Date modified: 1/28/2019 12:21 PM Date created: 1/28/2019 12:21 PM
Text Document Size: 8 bytes

Step 2:-

Open Access Data FTK. It will look as below :-



Step 3:-
Click on Evidence Tree ,Select Logical Drive & Click Next.



Please Select the Source Evidence Type

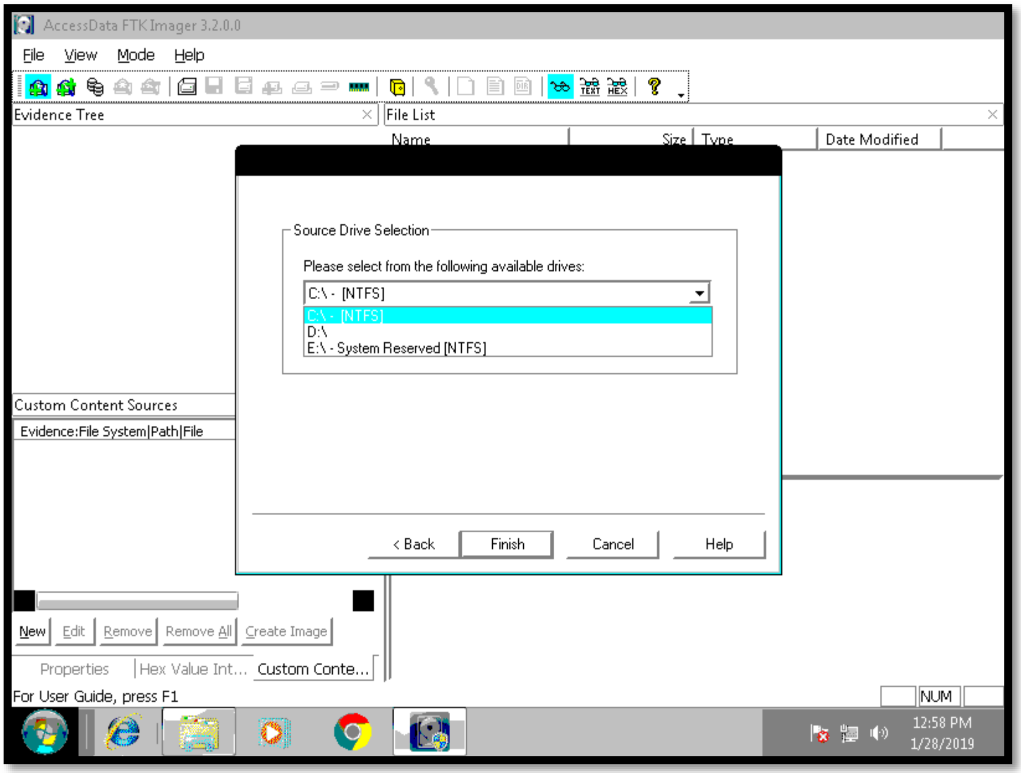
○ Physical Drive

● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Step 4:-
Select Source Drive.



Source Drive Selection

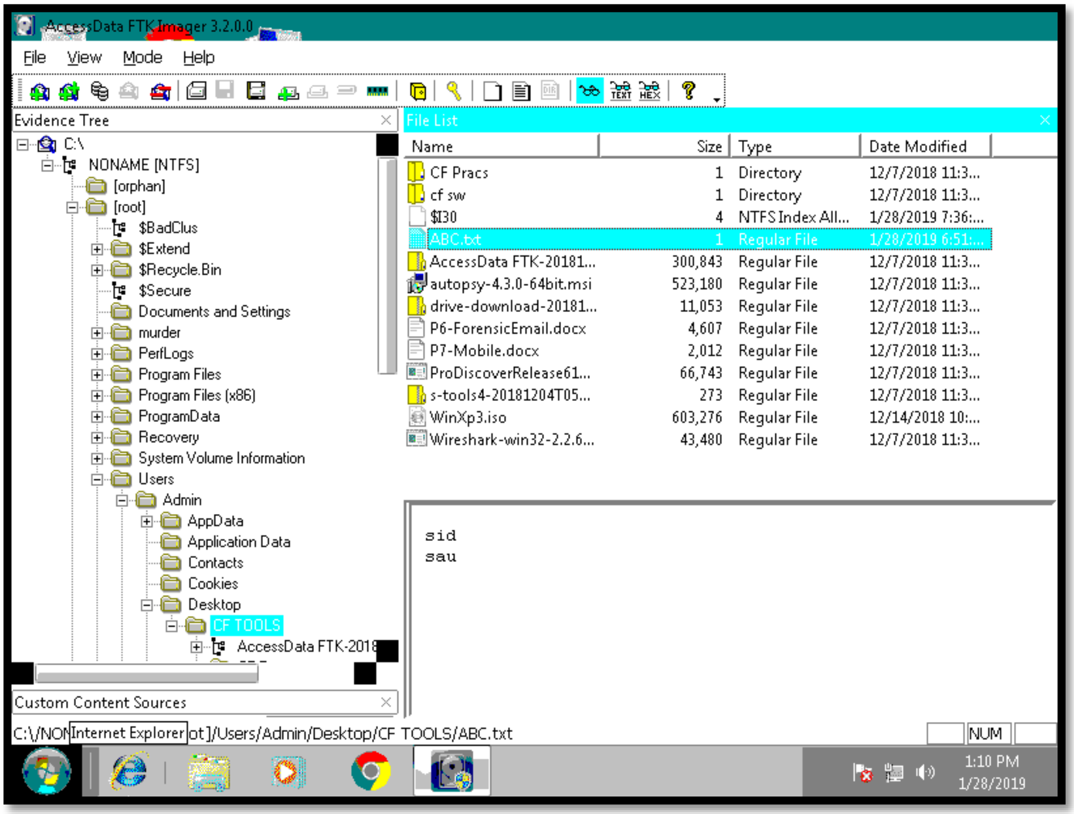
Please select from the following available drives:

C:\ - [NTFS]

C:\ - [NTFS]
D:\
E:\ - System Reserved [NTFS]

Step 5:-

Go to the path where you have stored the file. The File will Display in the file list.



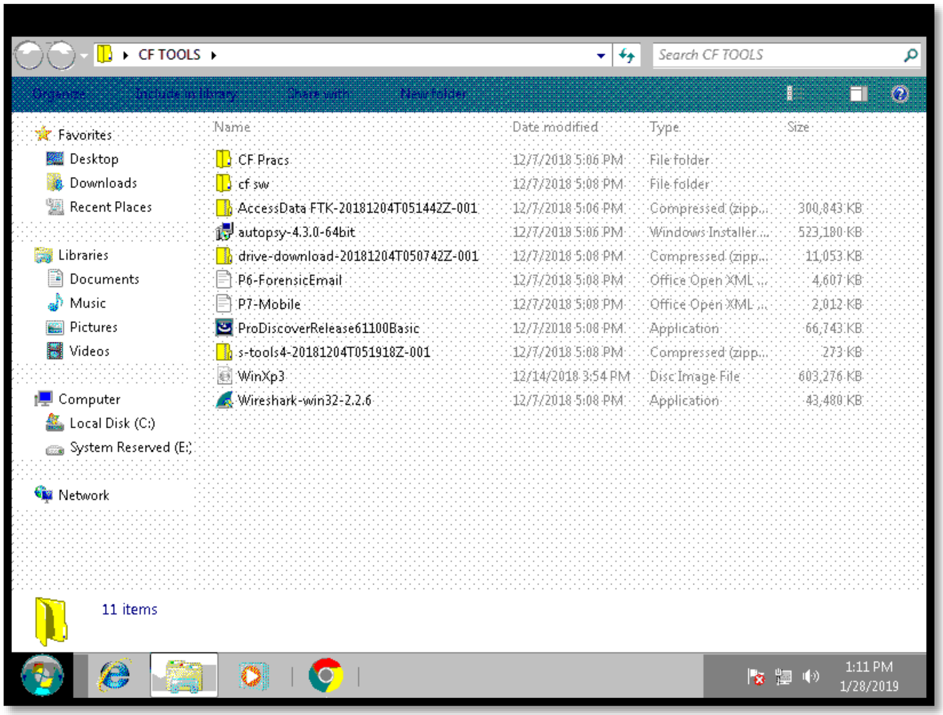
Name	Size	Type	Date Modified
CF Pracs	1	Directory	12/7/2018 11:3...
cf sw	1	Directory	12/7/2018 11:3...
$I30	4	NTFS Index All...	1/28/2019 7:36:...
ABC.txt	1	Regular File	1/28/2019 6:51:...
AccessData FTK-20181...	300,843	Regular File	12/7/2018 11:3...
autopsy-4.3.0-64bit.msi	523,180	Regular File	12/7/2018 11:3...
drive-download-20181...	11,053	Regular File	12/7/2018 11:3...
P6-ForensicEmail.docx	4,607	Regular File	12/7/2018 11:3...
P7-Mobile.docx	2,012	Regular File	12/7/2018 11:3...
ProDiscoverRelease61...	66,743	Regular File	12/7/2018 11:3...
s-tools4-20181204T05...	273	Regular File	12/7/2018 11:3...
WinXp3.iso	603,276	Regular File	12/14/2018 10:...
Wireshark-win32-2.2.6...	43,480	Regular File	12/7/2018 11:3...

```
sid
sau
```

C:\/NONInternet Explorerot]/Users/Admin/Desktop/CF TOOLS/ABC.txt

Step 6:-

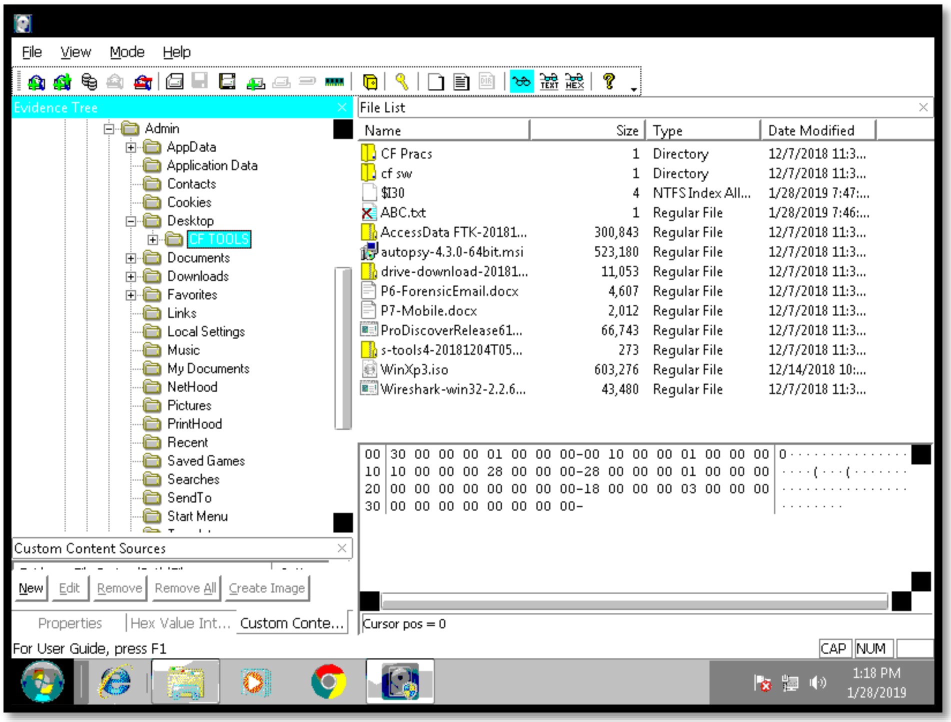
Now go to the folder again and delete the saved file.



Name	Date modified	Type	Size
CF Pracs	12/7/2018 5:06 PM	File folder	
cf sw	12/7/2018 5:08 PM	File folder	
AccessData FTK-20181204T051442Z-001	12/7/2018 5:06 PM	Compressed (zipp...	300,843 KB
autopsy-4.3.0-64bit	12/7/2018 5:06 PM	Windows Installer ...	523,180 KB
drive-download-20181204T050742Z-001	12/7/2018 5:08 PM	Compressed (zipp...	11,053 KB
P6-ForensicEmail	12/7/2018 5:08 PM	Office Open XML ...	4,607 KB
P7-Mobile	12/7/2018 5:08 PM	Office Open XML ...	2,012 KB
ProDiscoverRelease61100Basic	12/7/2018 5:08 PM	Application	66,743 KB
s-tools4-20181204T051918Z-001	12/7/2018 5:08 PM	Compressed (zipp...	273 KB
WinXp3	12/14/2018 3:54 PM	Disc Image File	603,276 KB
Wireshark-win32-2.2.6	12/7/2018 5:08 PM	Application	43,480 KB

Step 7:-

Open Access File FTK and walk through the path where you have stored the file. The File will be Displayed with a Cross mark.



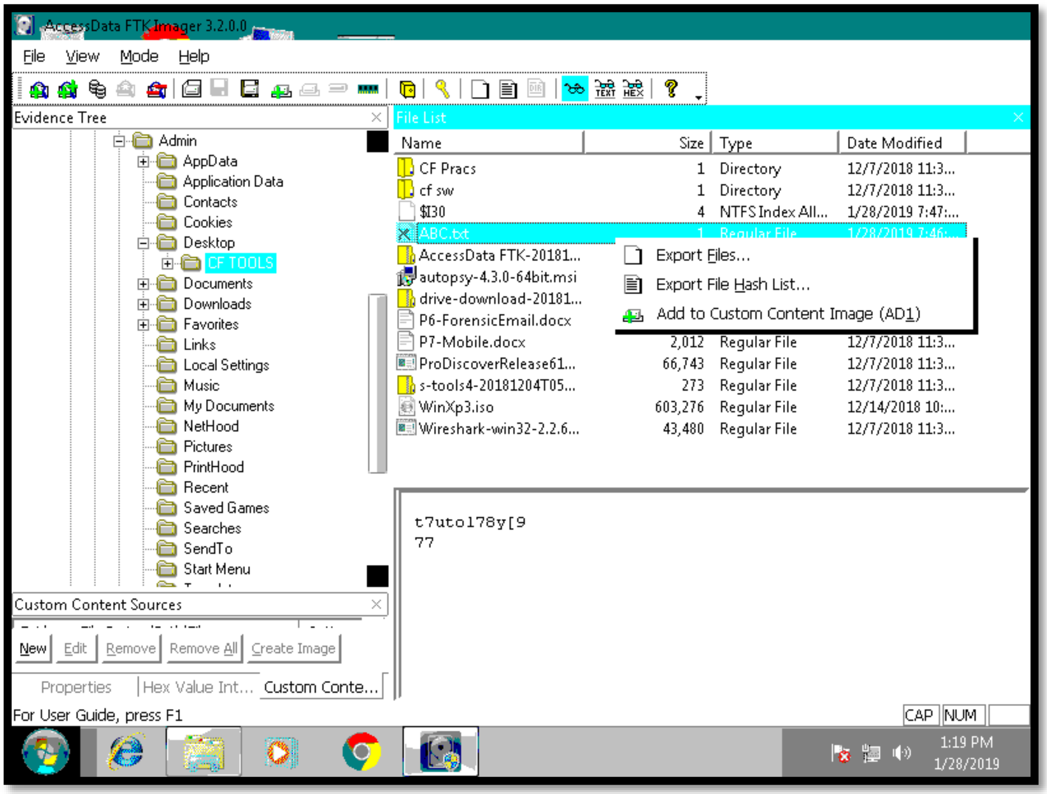
Name	Size	Type	Date Modified
CF Pracs	1	Directory	12/7/2018 11:3...
cf sw	1	Directory	12/7/2018 11:3...
$I30	4	NTFS Index All...	1/28/2019 7:47:...
ABC.txt	1	Regular File	1/28/2019 7:46:...
AccessData FTK-20181...	300,843	Regular File	12/7/2018 11:3...
autopsy-4.3.0-64bit.msi	523,180	Regular File	12/7/2018 11:3...
drive-download-20181...	11,053	Regular File	12/7/2018 11:3...
P6-ForensicEmail.docx	4,607	Regular File	12/7/2018 11:3...
P7-Mobile.docx	2,012	Regular File	12/7/2018 11:3...
ProDiscoverRelease61...	66,743	Regular File	12/7/2018 11:3...
s-tools4-20181204T05...	273	Regular File	12/7/2018 11:3...
WinXp3.iso	603,276	Regular File	12/14/2018 10:...
Wireshark-win32-2.2.6...	43,480	Regular File	12/7/2018 11:3...

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00  0···············
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00  ····(···(·······
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00  ················
30 00 00 00 00 00 00 00 00-                         ········
```

Cursor pos = 0

Step 8:-

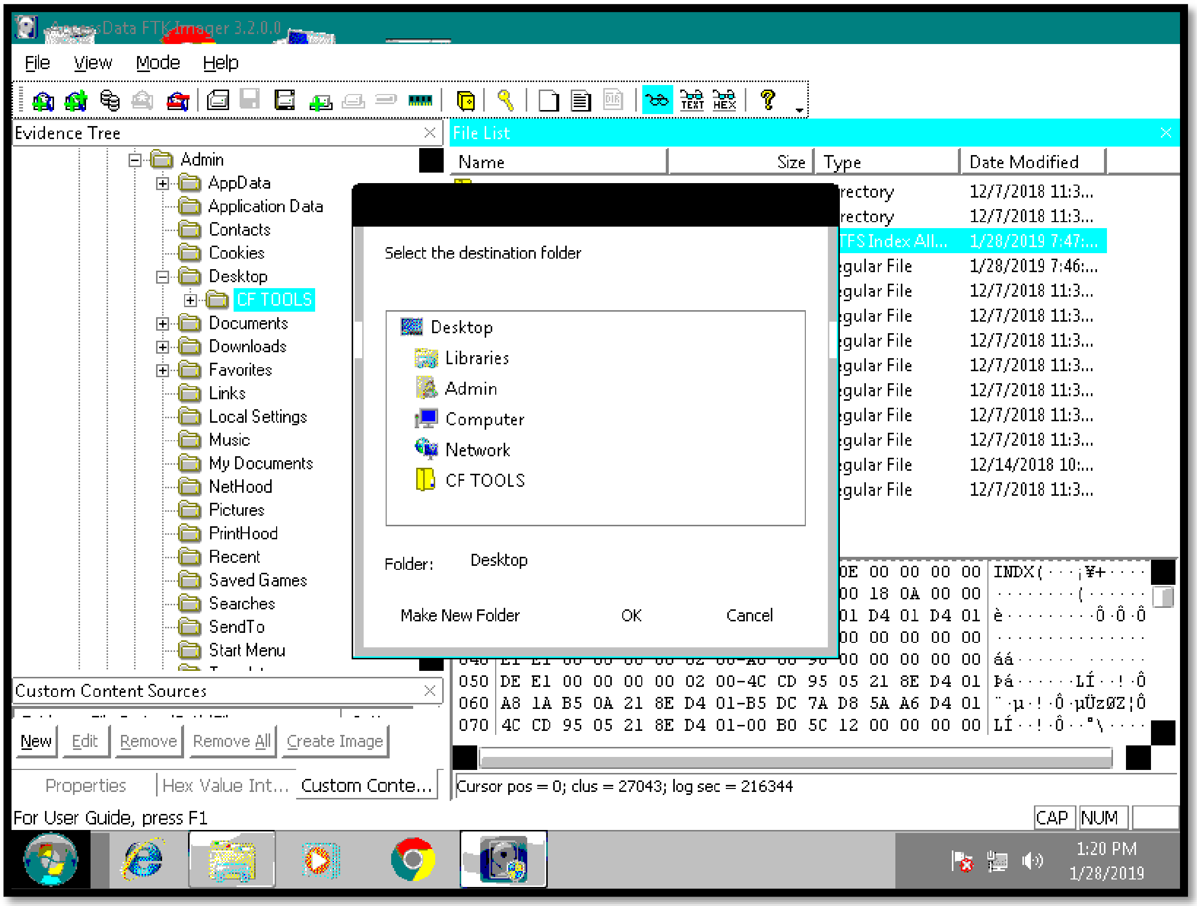
To Restore File Right Click on it And Select Export File Option.



Name	Size	Type	Date Modified
CF Pracs	1	Directory	12/7/2018 11:3...
cf sw	1	Directory	12/7/2018 11:3...
$I30	4	NTFS Index All...	1/28/2019 7:47:...
ABC.txt	1	Regular File	1/28/2019 7:46:...
AccessData FTK-20181...			
autopsy-4.3.0-64bit.msi			
drive-download-20181...			
P6-ForensicEmail.docx			
P7-Mobile.docx	2,012	Regular File	12/7/2018 11:3...
ProDiscoverRelease61...	66,743	Regular File	12/7/2018 11:3...
s-tools4-20181204T05...	273	Regular File	12/7/2018 11:3...
WinXp3.iso	603,276	Regular File	12/14/2018 10:...
Wireshark-win32-2.2.6...	43,480	Regular File	12/7/2018 11:3...

```
t7uto178y[9
77
```

Step 9:-
Select the path where the file to be exported.



Select the destination folder

Folder: Desktop

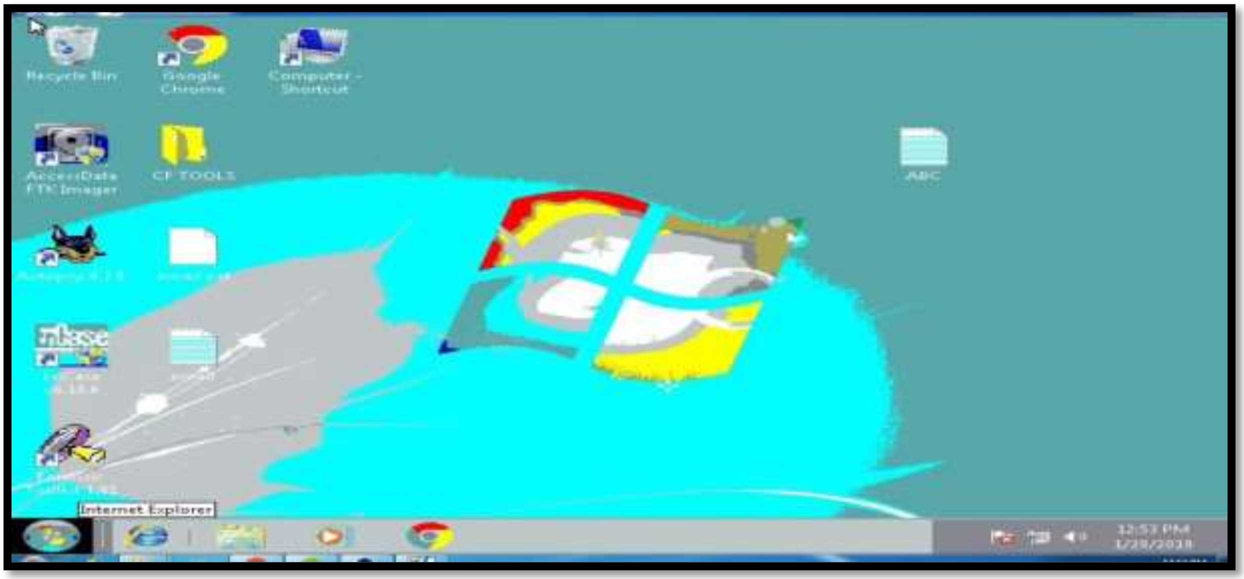
Type	Date Modified
rectory	12/7/2018 11:3...
rectory	12/7/2018 11:3...
TFS Index All...	1/28/2019 7:47:...
gular File	1/28/2019 7:46:...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/7/2018 11:3...
gular File	12/14/2018 10:...
gular File	12/7/2018 11:3...

```
0E 00 00 00 00  INDX(···¡¥+····
00 18 0A 00 00  ········(······
01 D4 01 D4 01  è·········Ô·Ô·Ô
00 00 00 00 00  ···············
00 00 00 00 00  áá·····  ······
050 DE E1 00 00 00 00 02 00-4C CD 95 05 21 8E D4 01  Þá······LÍ··!·Ô
060 A8 1A B5 0A 21 8E D4 01-B5 DC 7A D8 5A A6 D4 01  ¨·µ·!·Ô·µÜzØZ¦Ô
070 4C CD 95 05 21 8E D4 01-00 B0 5C 12 00 00 00 00  LÍ··!·Ô··°\····
```

Cursor pos = 0; clus = 27043; log sec = 216344

For User Guide, press F1

Step 10:-
File Will Be Restored.



CONCLUSION:- We successfully recovered and analyzed deleted data using FTK

PRACTICAL NO. 7

Aim:

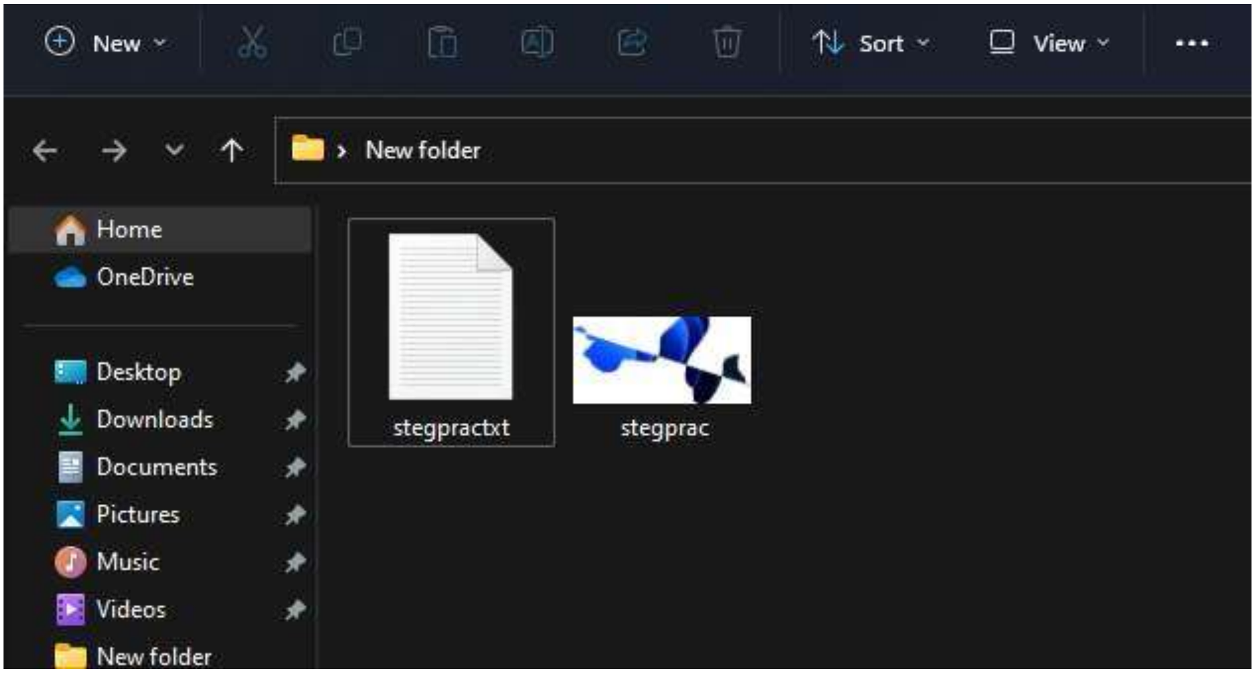
Steganography Detection

- Detect hidden information or files within digital images using steganography analysis tools.
- Extract and examine the hidden content.

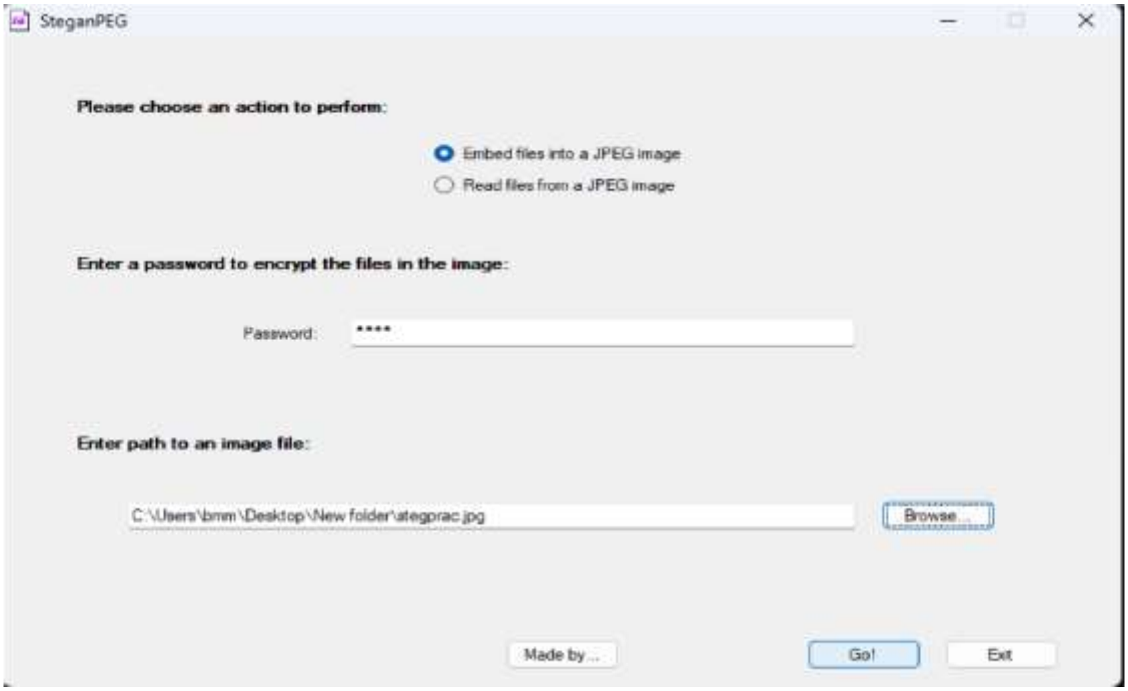
Practical:

In this Practical we going to use **SteganPeg** to check the hidden files in the given Image

Create a folder to keep the image and message file and store the txt file and image:



Open the SteganPEG and give a password and browse the path of the image



Please choose an action to perform:

● Embed files into a JPEG image

○ Read files from a JPEG image

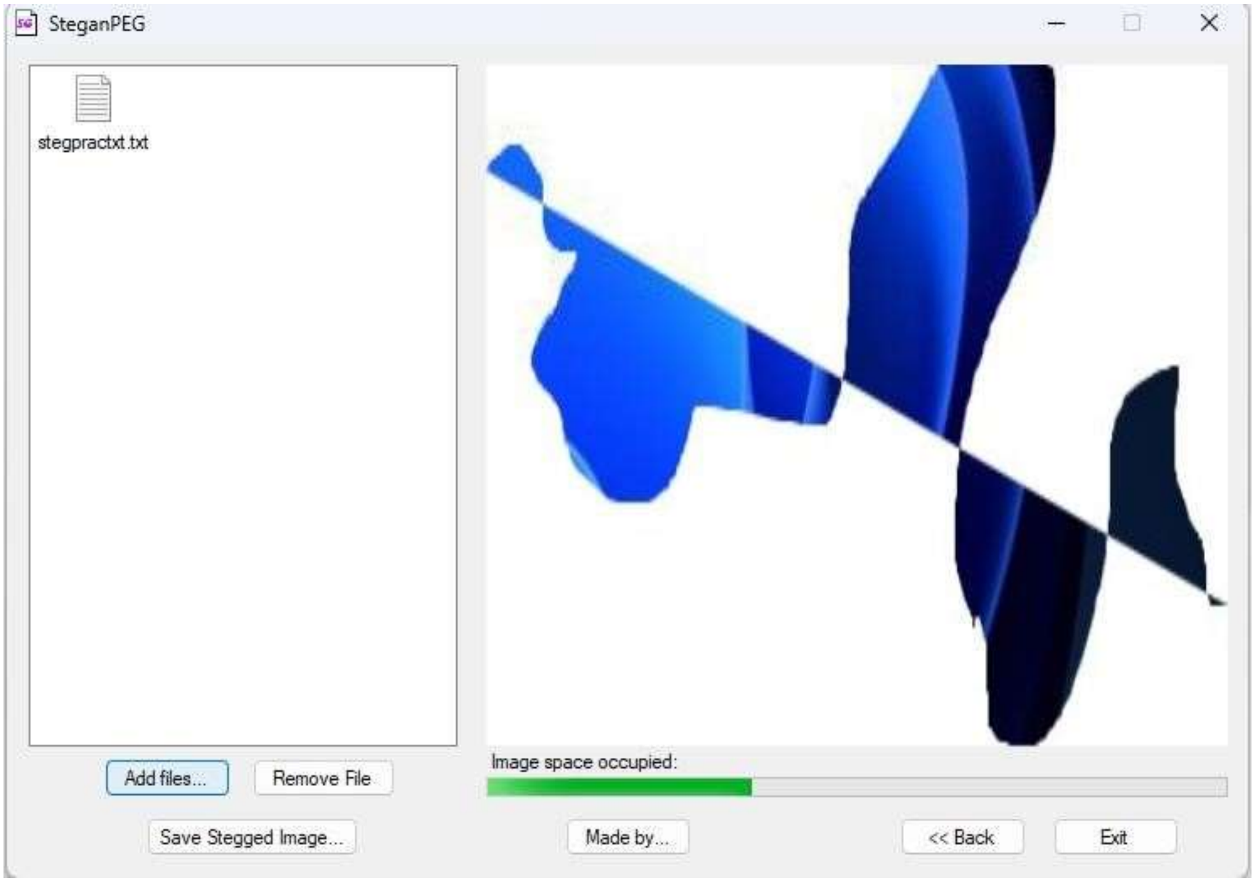
Enter a password to encrypt the files in the image:

Password: ****

Enter path to an image file:

C:\Users\bmm\Desktop\New folder\stegprac.jpg

First we are going to add some files in the captured image



stegpractxt.txt

Image space occupied:

Save the stegged image

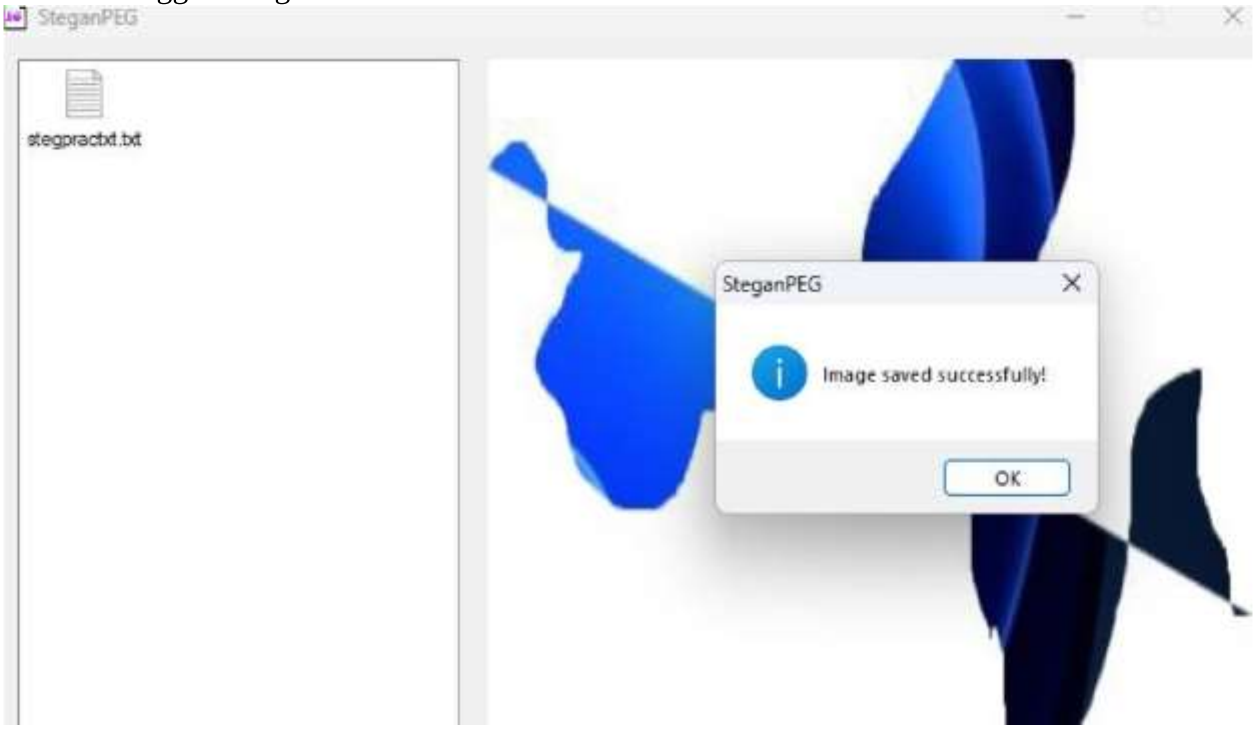
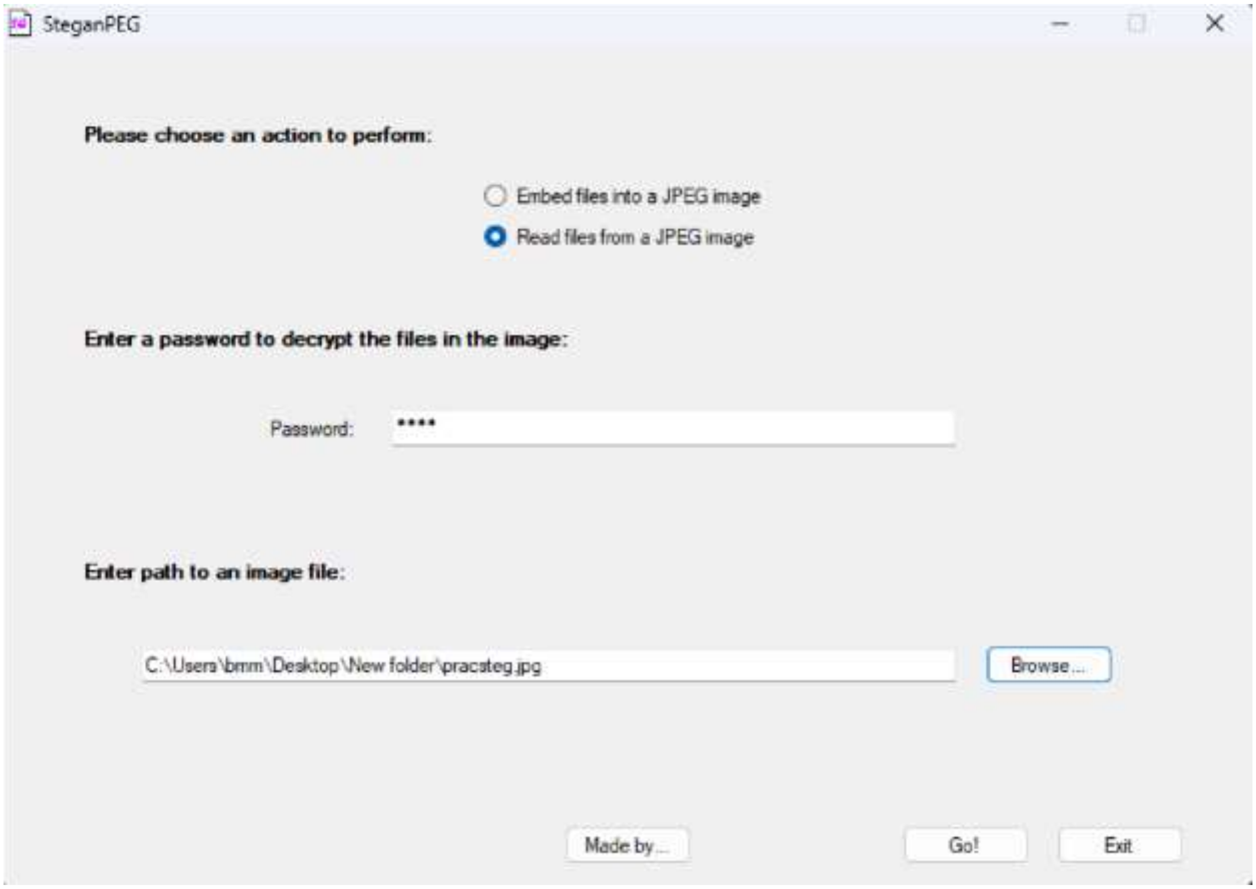


Image saved successfully!

Open the saved image with the assigned password and view the image with hidden files



Please choose an action to perform:

○ Embed files into a JPEG image

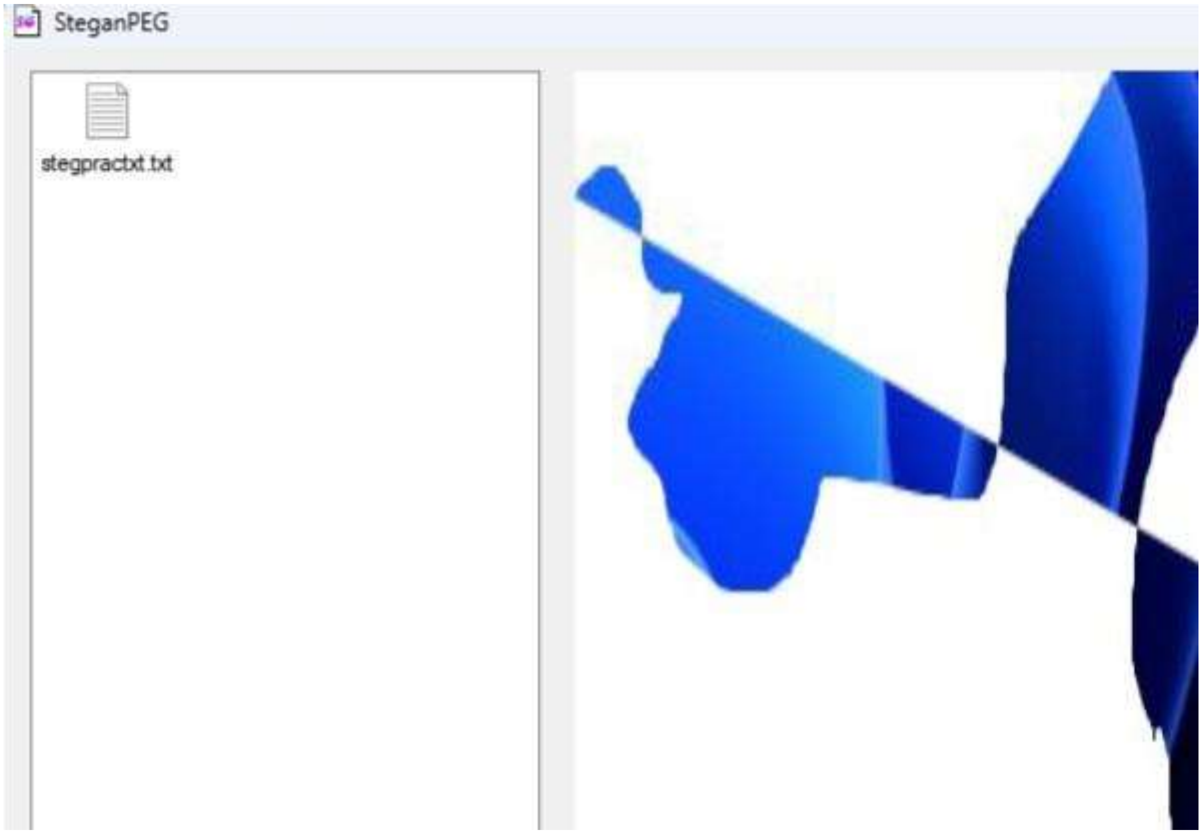
● Read files from a JPEG image

Enter a password to decrypt the files in the image:

Password: ****

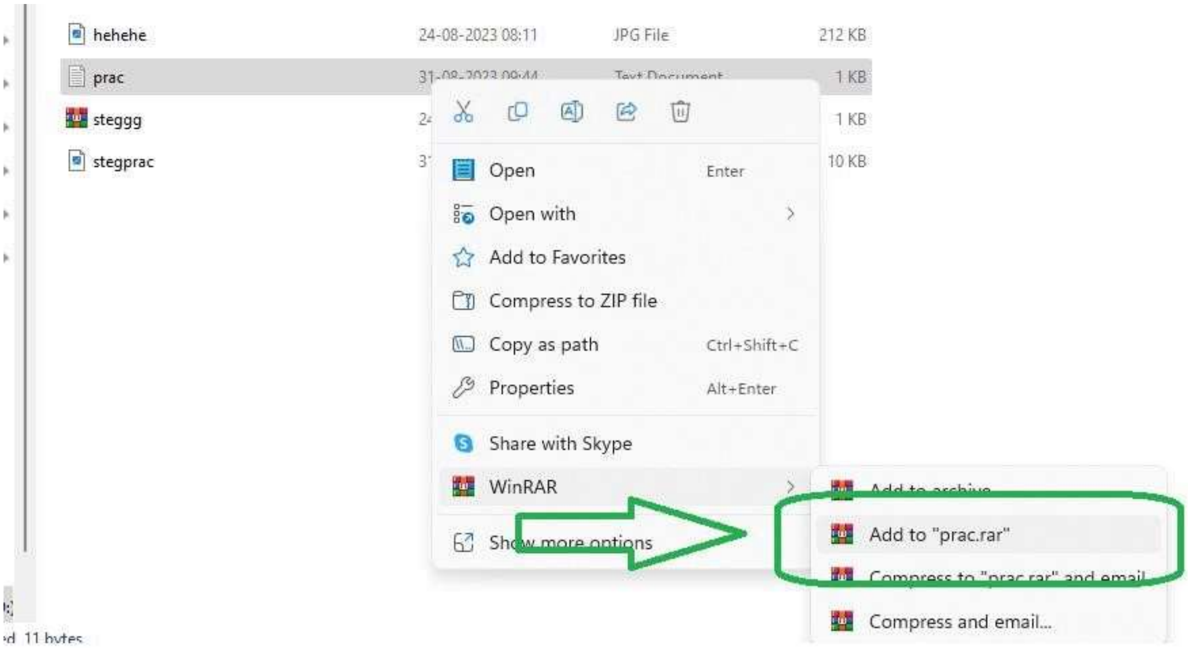
Enter path to an image file:

C:\Users\bmm\Desktop\New folder\pracsteg.jpg



Now we are going to do the **stegging process** using **Command Prompt** and **viewing** the Image using the **WinRAR**

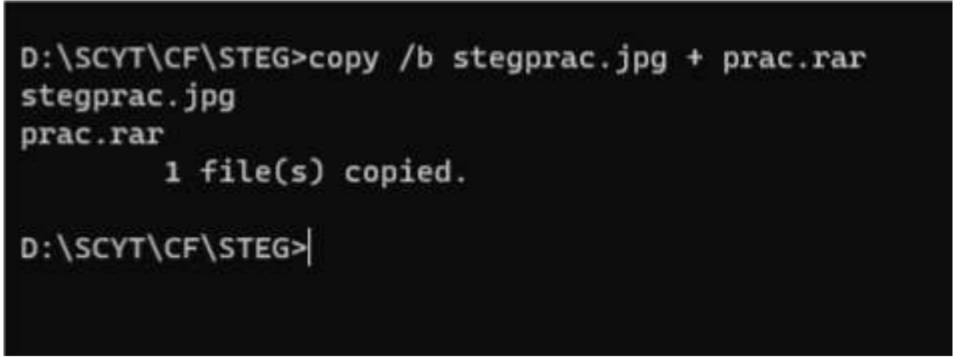
Make a zip file of the text file



hehehe	24-08-2023 08:11	JPG File	212 KB
prac	31-08-2023 09:44	Text Document	1 KB
steggg	24		1 KB
stegprac	31		10 KB

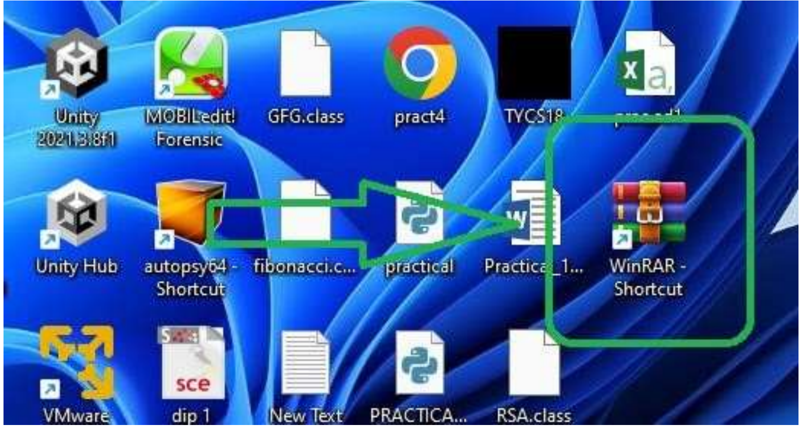
Go to **Command Prompt** and **Type** the **Syntax**

:\Users\ROYAL\Desktop\New Folder>copy/b stegprac.jpg + stegpractxt.rar



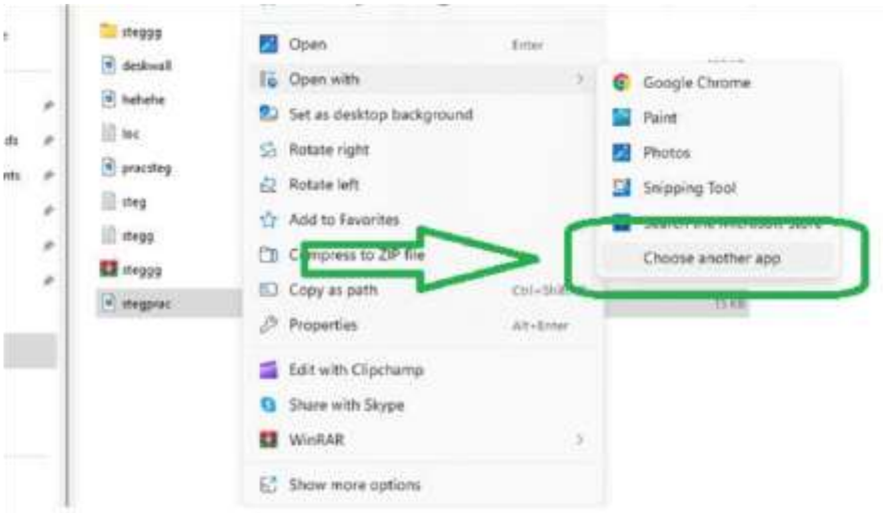
```
D:\SCYT\CF\STEG>copy /b stegprac.jpg + prac.rar
stegprac.jpg
prac.rar
        1 file(s) copied.

D:\SCYT\CF\STEG>
```

Then create a shortcut for WinRAR on the desktop

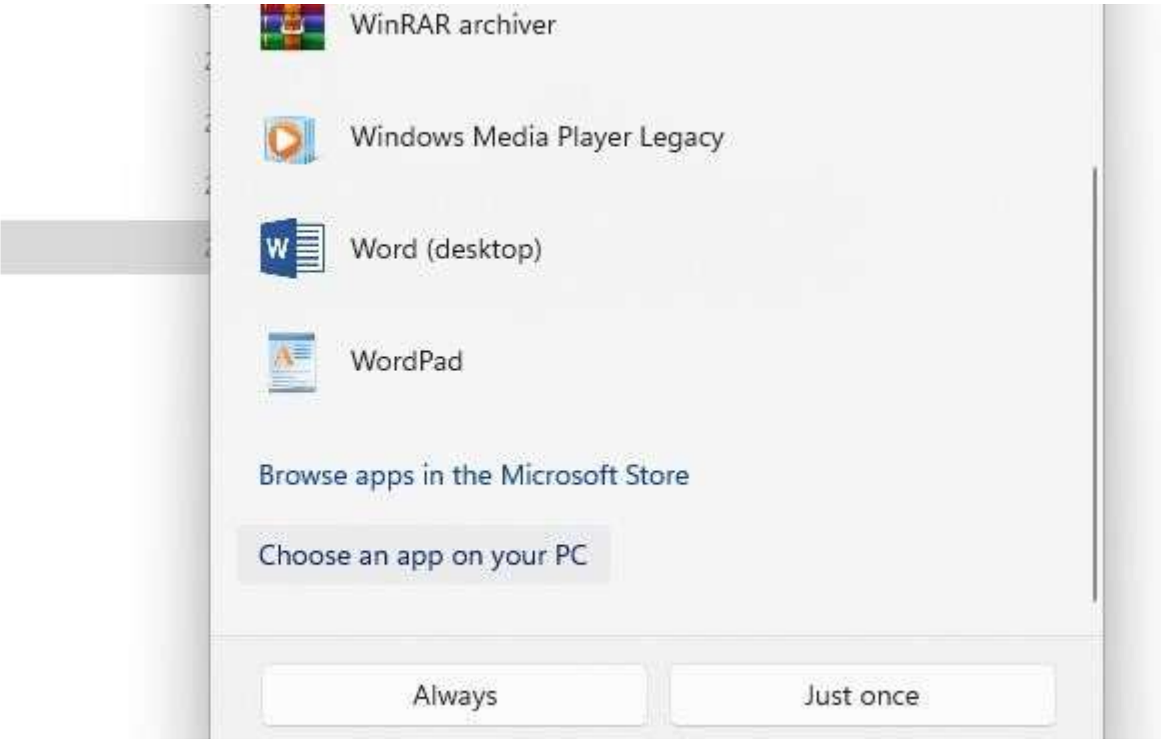


Then open the image using the shortcut

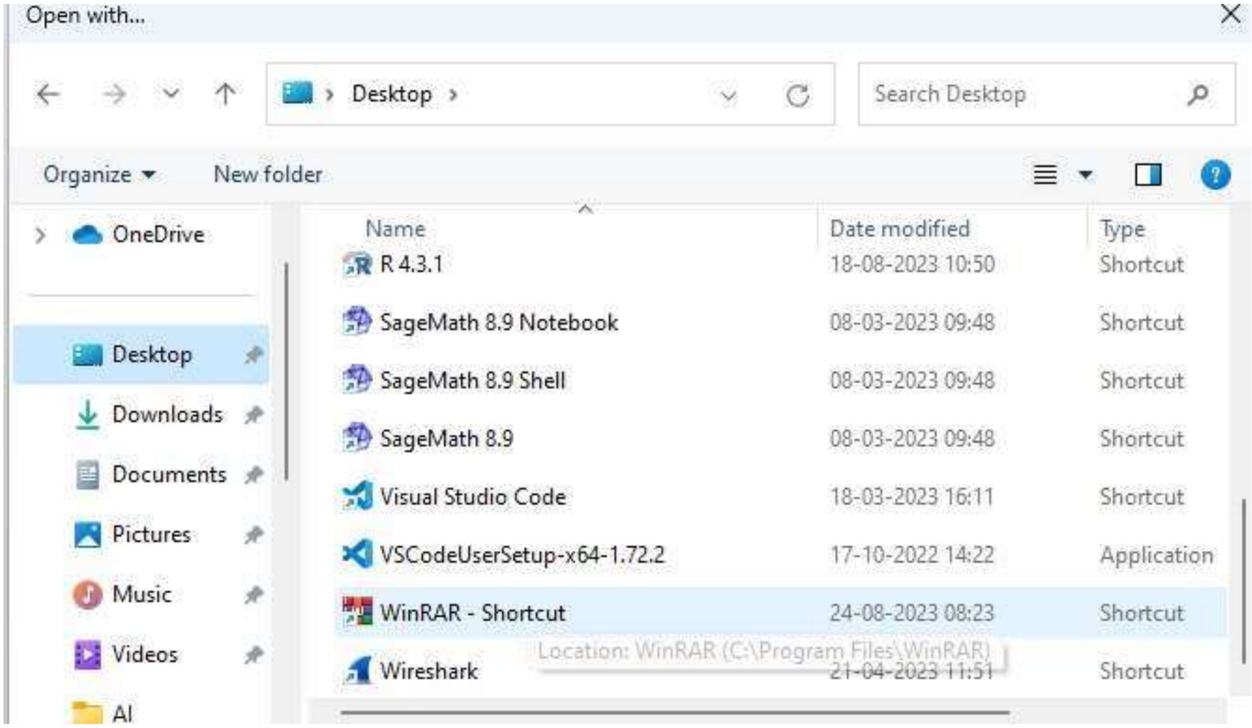
Right Click on the image □ **Open with** □ **Choose another app**



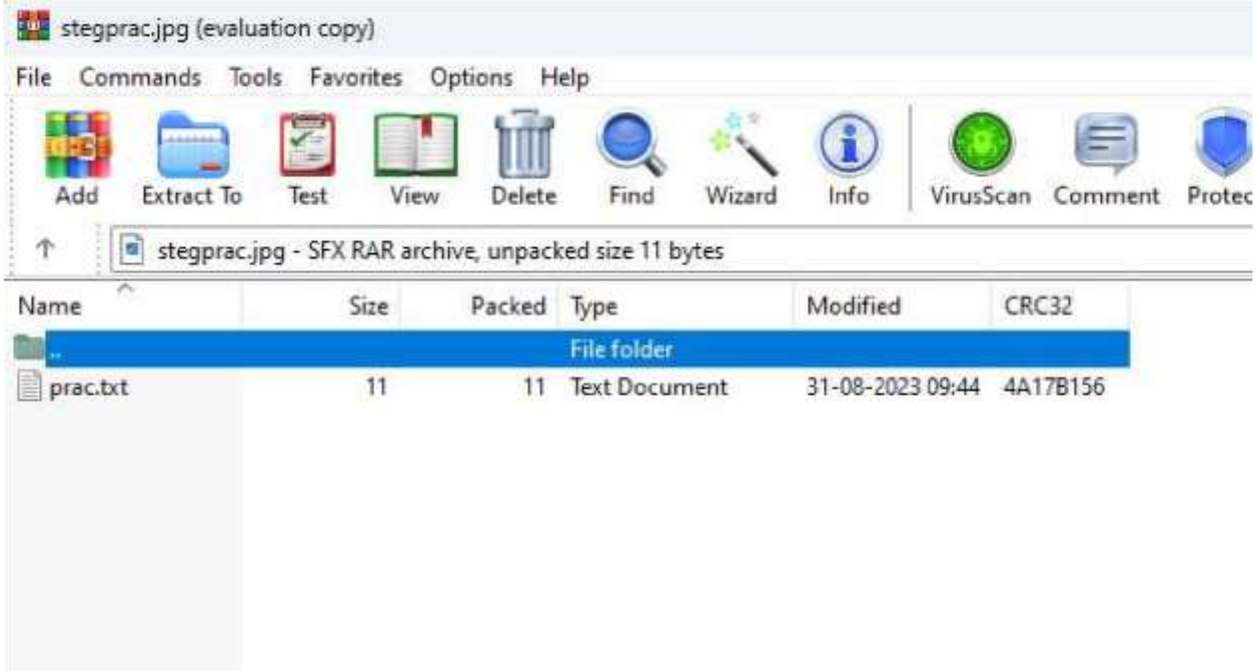
Select **Choose another app** □ **choose an app on your pc**



Then **Desktop** □ **Shortcut created of WinRAR** and **Select Just Once**



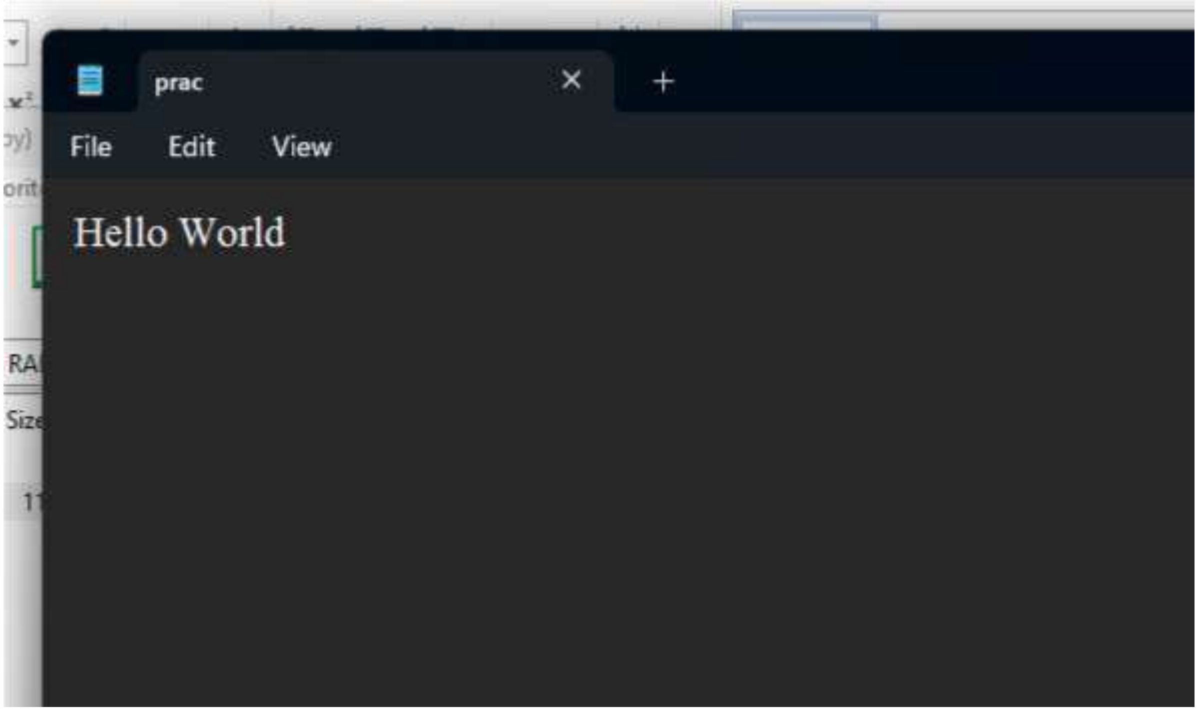
Name	Date modified	Type
R 4.3.1	18-08-2023 10:50	Shortcut
SageMath 8.9 Notebook	08-03-2023 09:48	Shortcut
SageMath 8.9 Shell	08-03-2023 09:48	Shortcut
SageMath 8.9	08-03-2023 09:48	Shortcut
Visual Studio Code	18-03-2023 16:11	Shortcut
VSCodeUserSetup-x64-1.72.2	17-10-2022 14:22	Application
WinRAR - Shortcut	24-08-2023 08:23	Shortcut
Wireshark	21-04-2023 11:51	Shortcut



stegprac.jpg - SFX RAR archive, unpacked size 11 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
prac.txt	11	11	Text Document	31-08-2023 09:44	4A17B156

View the Extracted File



Hello World

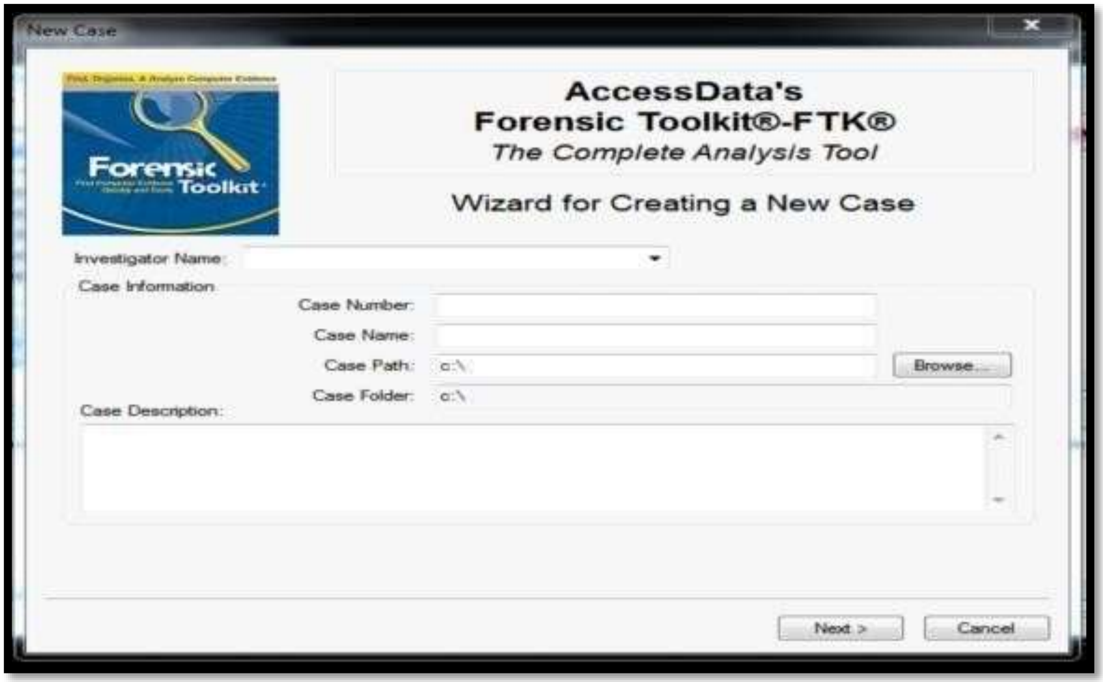
Practical 8

Email Forensics

- You First Required a .pst file in Your Computer As Evidence
- A .pst file is A Backup of Your Microsoft Outlook Account Mails

To Perform Recovery of Deleted Mails From .pst file required FTK (Forensic Toolkit)

1. Install Access Data FTK and Open it
2. Enter Details



Investigator Name:

Case Information

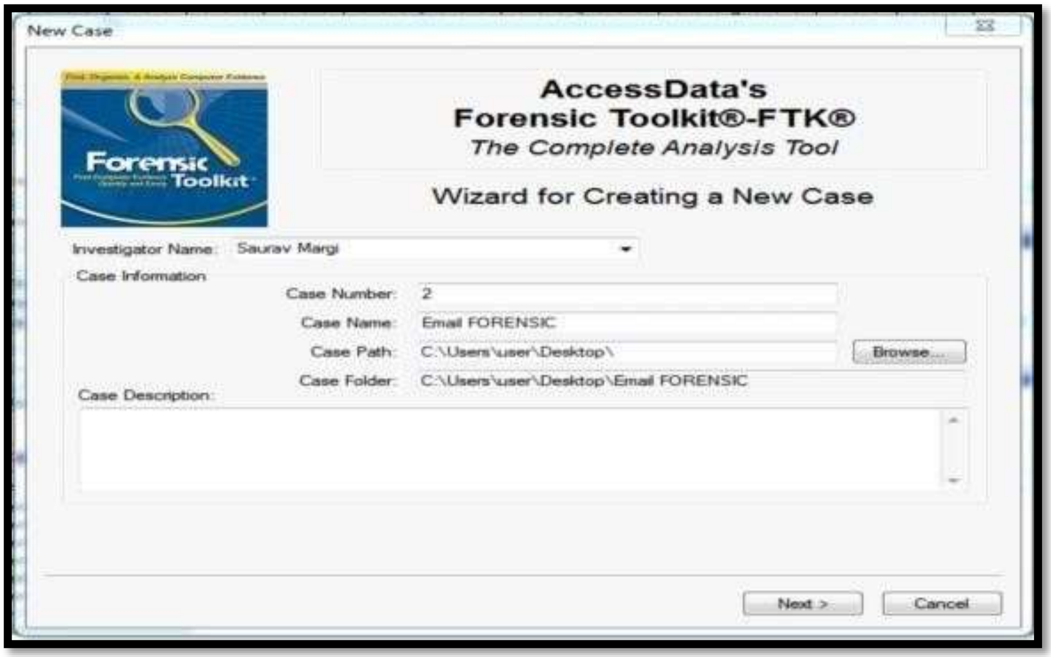
Case Number:

Case Name:

Case Path: c:\

Case Folder: c:\

Case Description:



Investigator Name: Saurav Margi

Case Information

Case Number: 2

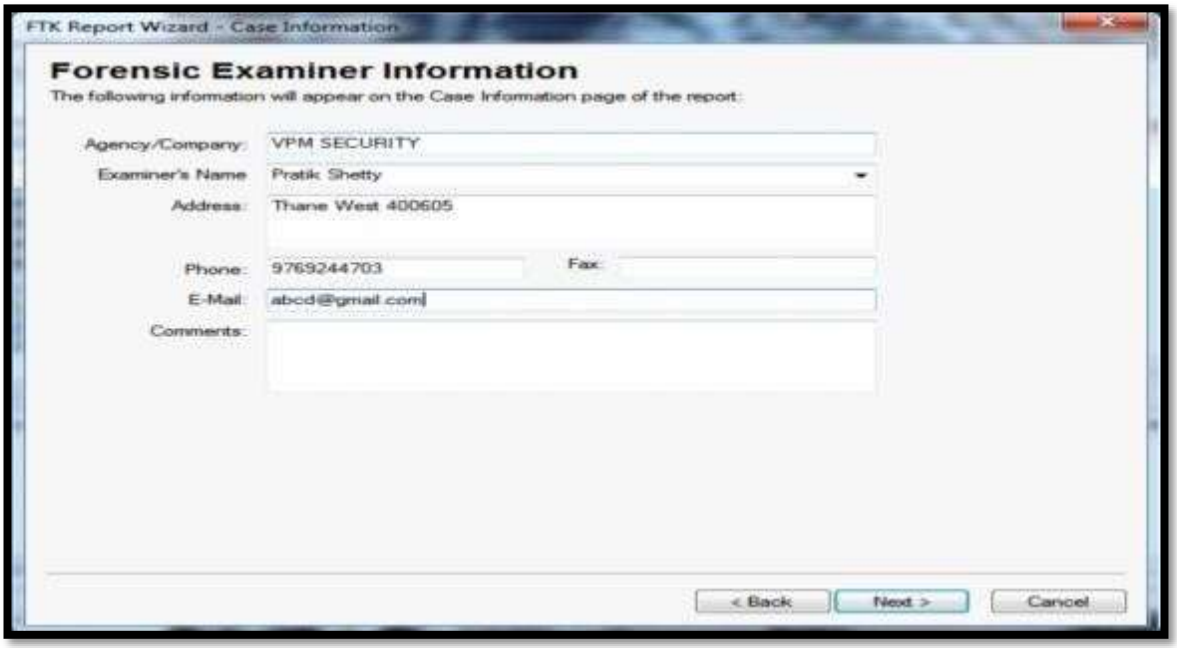
Case Name: Email FORENSIC

Case Path: C:\Users\user\Desktop\

Case Folder: C:\Users\user\Desktop\Email FORENSIC

Case Description:

3. Enter Forensic Examiners Information



Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company: VPM SECURITY

Examiner's Name: Pratik Shetty

Address: Thane West 400605

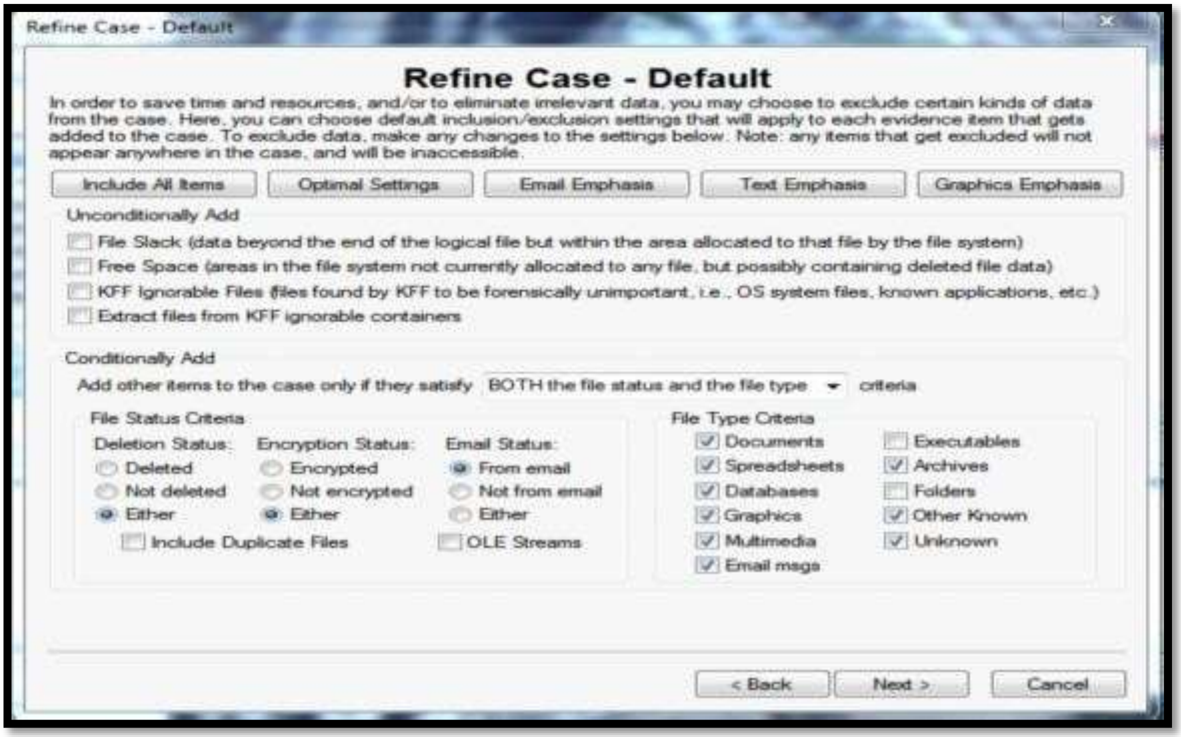
Phone: 9769244703

Fax:

E-Mail: abcd@gmail.com

Comments:

4. Refine Case Select Email Emphasis & Click Next



Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

Unconditionally Add

- □ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- □ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- □ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- □ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status: ○ Deleted ○ Not deleted ● Either

Encryption Status: ○ Encrypted ○ Not encrypted ● Either

Email Status: ● From email ○ Not from email ○ Either

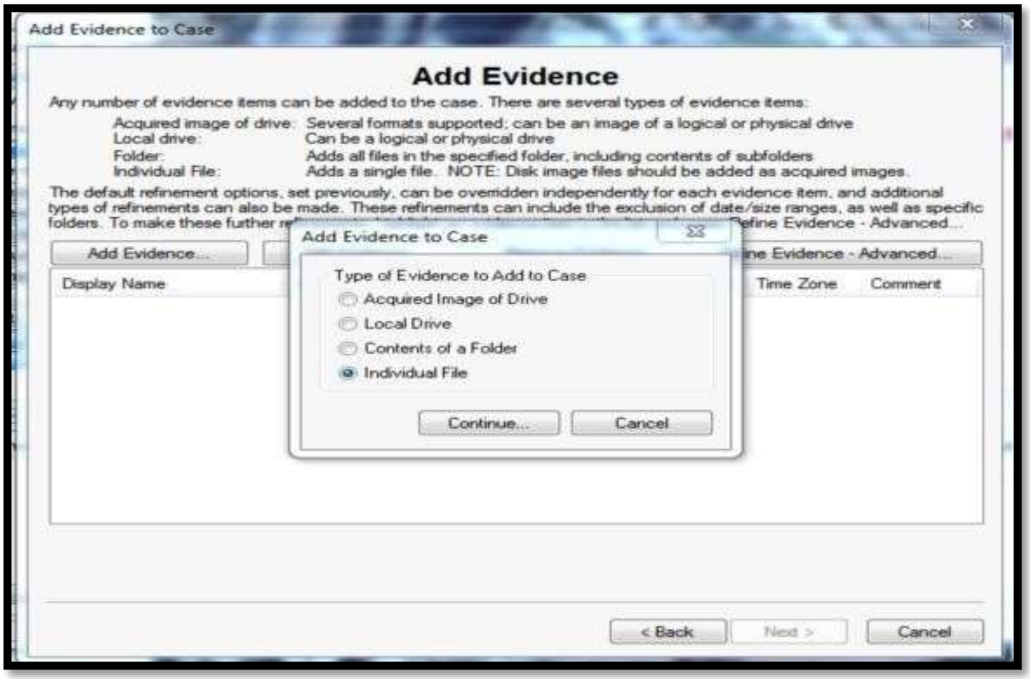
□ Include Duplicate Files

□ OLE Streams

File Type Criteria

☑ Documents	□ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	□ Folders
☑ Graphics	☑ Other Known
☑ Multimedia	☑ Unknown
☑ Email msgs	

5. Click Add Evidence And Select Evidence File Type



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further r

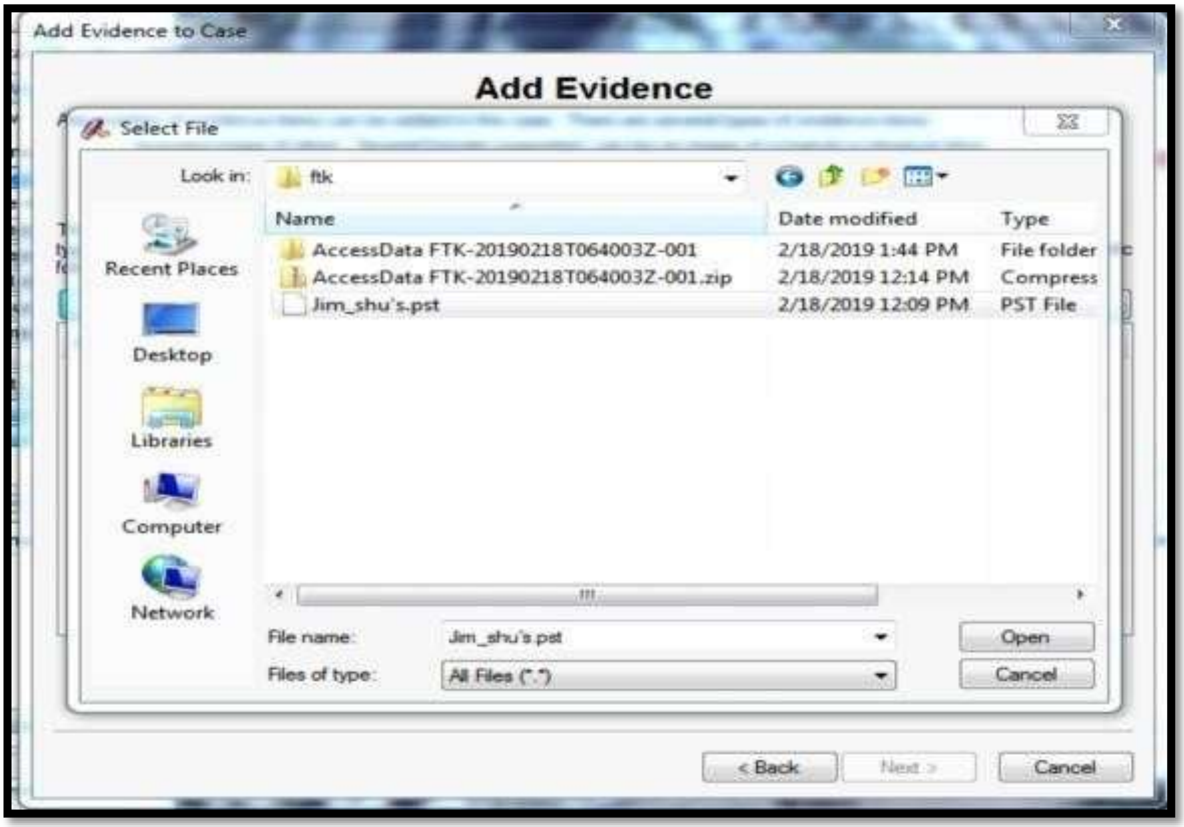
efine Evidence - Advanced...

Add Evidence to Case

Type of Evidence to Add to Case

○ Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
● Individual File

6. Select Evidence File



Add Evidence to Case

Add Evidence

Select File

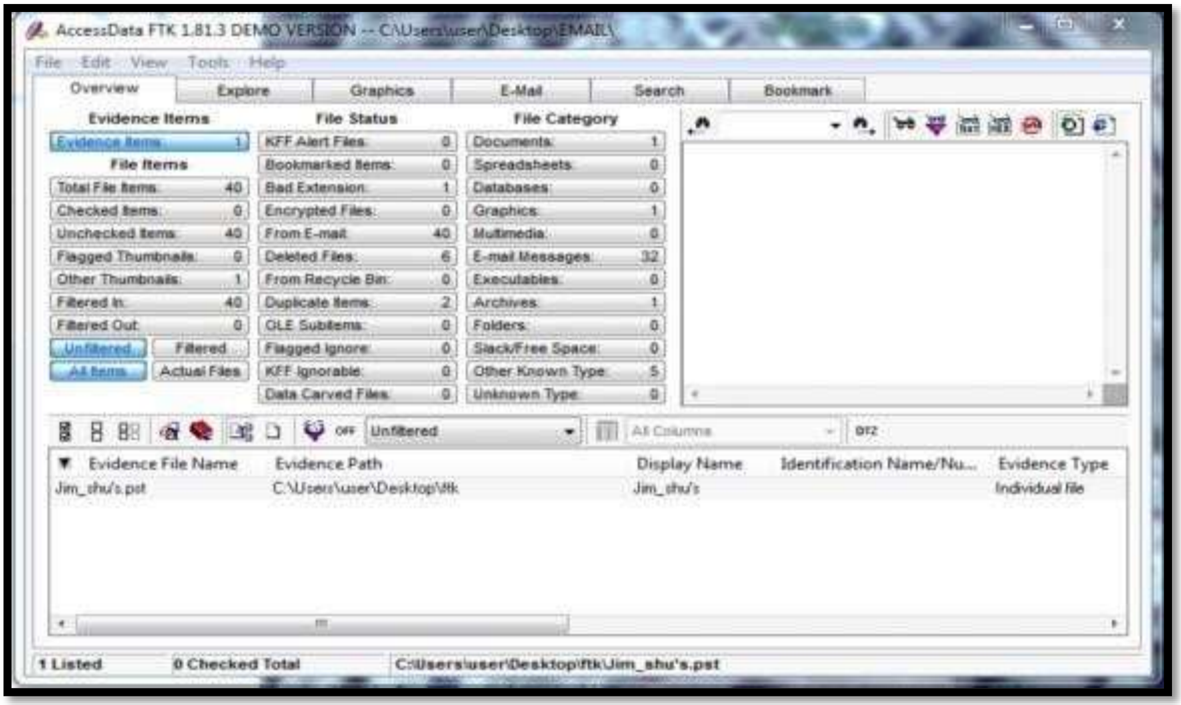
Look in: ftk

Name	Date modified	Type
AccessData FTK-20190218T064003Z-001	2/18/2019 1:44 PM	File folder
AccessData FTK-20190218T064003Z-001.zip	2/18/2019 12:14 PM	Compress
Jim_shu's.pst	2/18/2019 12:09 PM	PST File

File name: Jim_shu's.pst

Files of type: All Files (*.*)

7. Selected File Will Be Displayed In Access Data FTK



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	40	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	40	From E-mail:	40	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	6	E-mail Messages:	32
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	40	Duplicate Items:	2	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
		Flagged Ignore:	0	Slack/Free Space:	0
		KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

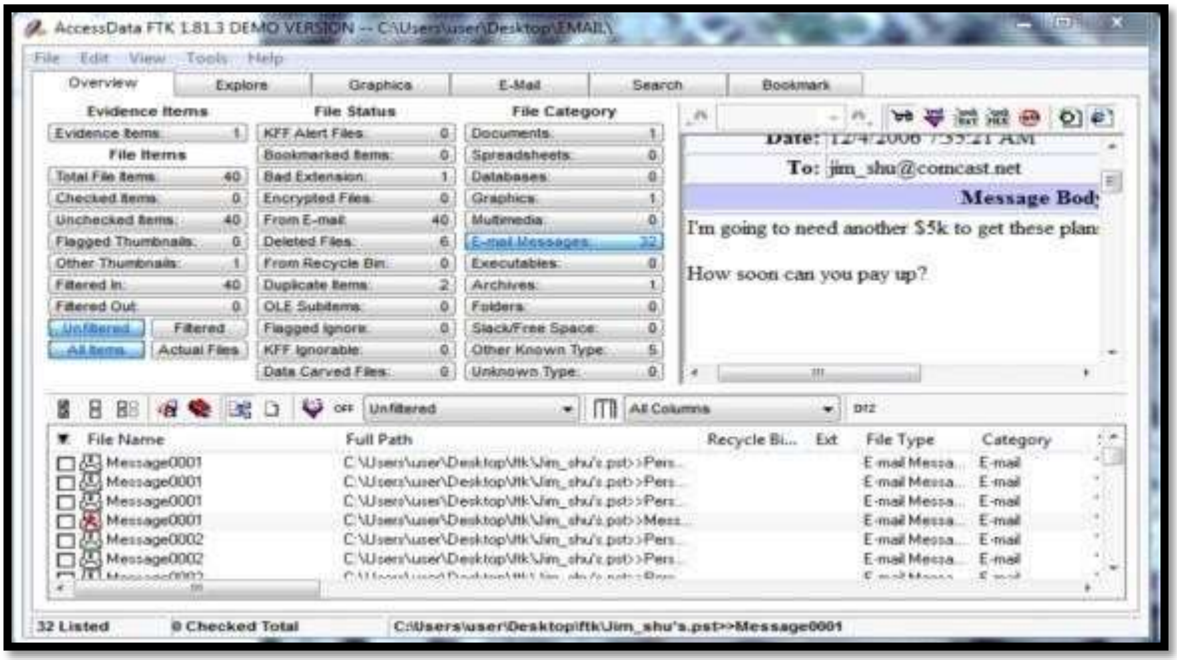
Unfiltered

All Columns

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evidence Type
Jim_shu's.pst	C:\Users\user\Desktop\ftk	Jim_shu's		Individual file

1 Listed | 0 Checked Total | C:\Users\user\Desktop\ftk\Jim_shu's.pst

8. Click on Email Messages To See Emails
Deleted Emails Are Shown In Red Cross Symbols



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	40	Bad Extension:	1	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	1
Unchecked Items:	40	From E-mail:	40	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	6	E-mail Messages:	32
Other Thumbnails:	1	From Recycle Bin:	0	Executables:	0
Filtered In:	40	Duplicate Items:	2	Archives:	1
Filtered Out:	0	OLE Subitems:	0	Folders:	0
		Flagged Ignore:	0	Slack/Free Space:	0
		KFF Ignorable:	0	Other Known Type:	5
		Data Carved Files:	0	Unknown Type:	0

Date: 12/4/2006 7:35:21 AM
To: jim_shu@comcast.net

Message Body

I'm going to need another $5k to get these plan

How soon can you pay up?

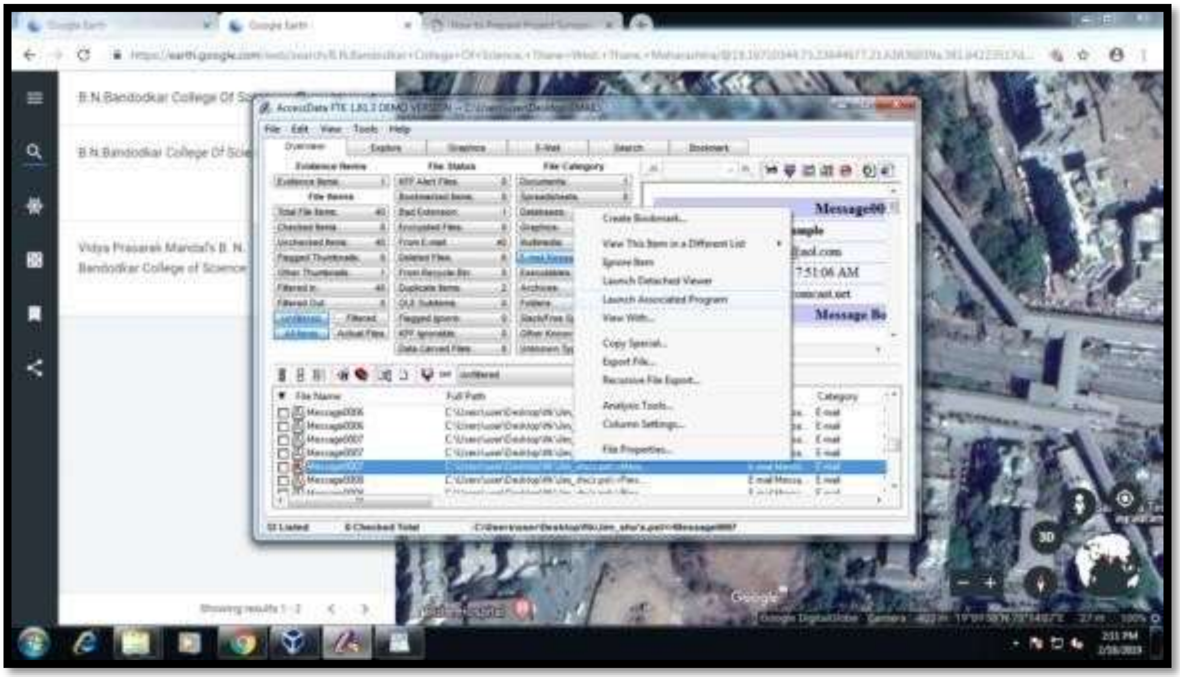
Unfiltered

All Columns

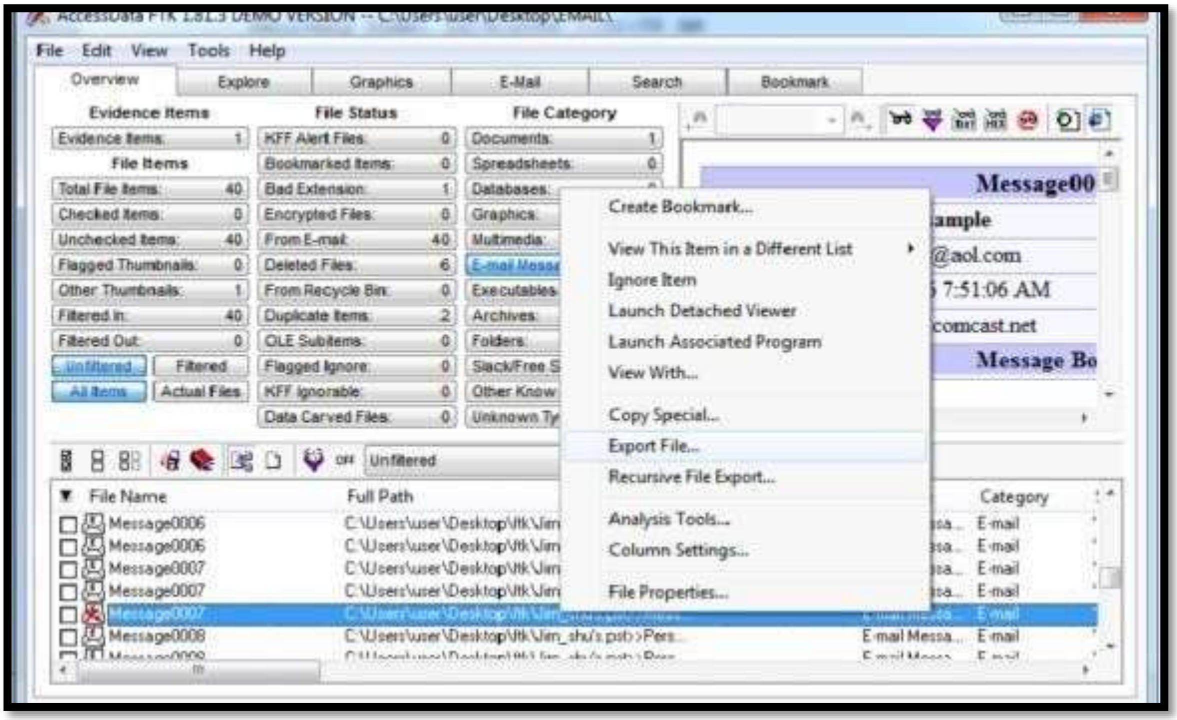
File Name	Full Path	Recycle Bi...	Ext	File Type	Category
□ Message0001	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...			E-mail Messa...	E-mail
□ Message0001	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...			E-mail Messa...	E-mail
□ Message0001	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...			E-mail Messa...	E-mail
□ Message0001	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Mess...			E-mail Messa...	E-mail
□ Message0002	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...			E-mail Messa...	E-mail
□ Message0002	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...			E-mail Messa...	E-mail

32 Listed | 0 Checked Total | C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Message0001

9. Right Click On Deleted Mails And Select Launch Associated Programs


AccessData FTK 1.81.3 DEMO VERSION -- C:\Users\user\Desktop\EMAIL\
Create Bookmark...
View This Item in a Different List
Ignore Item
Launch Detached Viewer
Launch Associated Program
View With...
Copy Special...
Export File...
Recursive File Export...
Analysis Tools...
Column Settings...
File Properties...
B.N.Bandodkar College Of Science
Vidya Prasarak Mandal's B. N. Bandodkar College of Science
Google

10. Or To Export Deleted Mail as an Individual File Right Click and Select Export File



Evidence Items

Evidence Items:	1

File Items

Total File Items:	40
Checked Items:	0
Unchecked Items:	40
Flagged Thumbnails:	0
Other Thumbnails:	1
Filtered In:	40
Filtered Out:	0

File Status

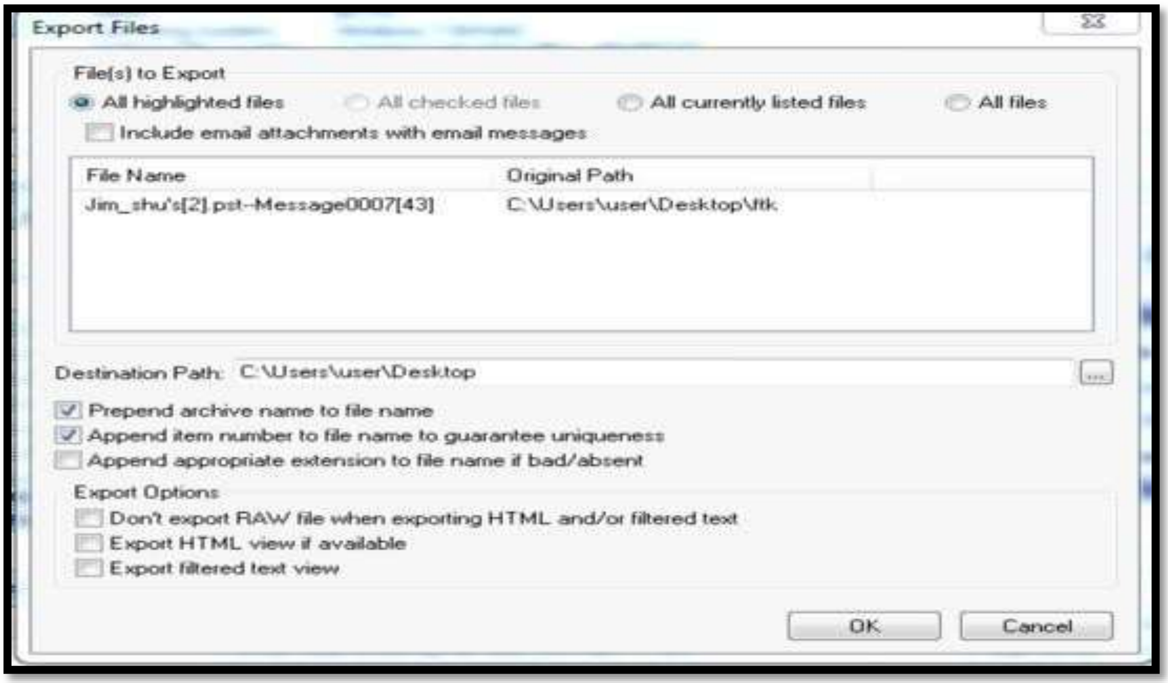
KFF Alert Files:	0
Bookmarked Items:	0
Bad Extension:	1
Encrypted Files:	0
From E-mail:	40
Deleted Files:	6
From Recycle Bin:	0
Duplicate Items:	2
OLE Subitems:	0
Flagged Ignore:	0
KFF Ignorable:	0
Data Carved Files:	0

File Category

Documents:	1
Spreadsheets:	0
Databases:	0
Graphics:	
Multimedia:	
E-mail Messa	
Executables:	
Archives:	
Folders:	
Slack/Free S	
Other Know	
Unknown Ty	

File Name	Full Path		Category
Message0006	C:\Users\user\Desktop\ftk\Jim	...sa...	E-mail
Message0006	C:\Users\user\Desktop\ftk\Jim	...sa...	E-mail
Message0007	C:\Users\user\Desktop\ftk\Jim	...sa...	E-mail
Message0007	C:\Users\user\Desktop\ftk\Jim	...sa...	E-mail
Message0007	C:\Users\user\Desktop\ftk\Jim	E-mail Messa...	E-mail
Message0008	C:\Users\user\Desktop\ftk\Jim_shu's.pst>>Pers...	E-mail Messa...	E-mail

11. Select Path For File To Be Exported.



Export Files

File(s) to Export

● All highlighted files ○ All checked files ○ All currently listed files ○ All files

□ Include email attachments with email messages

File Name	Original Path
Jim_shu's[2].pst-Message0007[43]	C:\Users\user\Desktop\ftk

Destination Path: C:\Users\user\Desktop

☑ Prepend archive name to file name

☑ Append item number to file name to guarantee uniqueness

□ Append appropriate extension to file name if bad/absent

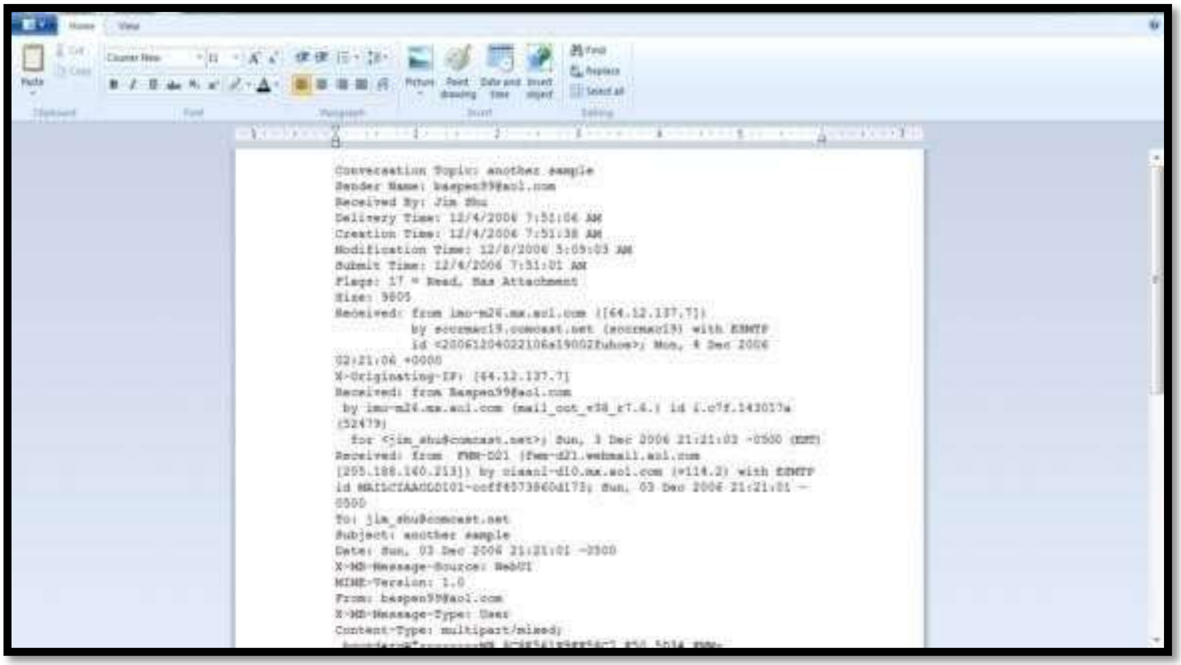
Export Options

□ Don't export RAW file when exporting HTML and/or filtered text

□ Export HTML view if available

□ Export filtered text view

12. Select Any Program to View File We Selected WordPad.



```
Conversation Topic: another sample
Sender Name: baspen99@aol.com
Received By: Jim Shu
Delivery Time: 12/4/2006 7:51:06 AM
Creation Time: 12/4/2006 7:51:38 AM
Modification Time: 12/8/2006 5:09:03 AM
Submit Time: 12/4/2006 7:51:01 AM
Flags: 17 = Read, Has Attachment
Size: 9805
Received: from imo-m26.mx.aol.com ([64.12.137.7])
          by sccrmxc19.comcast.net (sccrmxc19) with ESMTP
          id <20061204022106s19002fuhoe>; Mon, 4 Dec 2006
02:21:06 +0000
X-Originating-IP: [64.12.137.7]
Received: from Baspen99@aol.com
 by imo-m26.mx.aol.com (mail_out_v38_r7.6.) id i.c7f.143017a
(52479)
  for <jim_shu@comcast.net>; Sun, 3 Dec 2006 21:21:03 -0500 (EST)
Received: from  FWM-D21 (fwm-d21.webmail.aol.com
[205.188.160.213]) by cia-aol-d10.mx.aol.com (v114.2) with ESMTP
id MAILCIAAOLD101-ccff4573960d173; Sun, 03 Dec 2006 21:21:01 -
0500
To: jim_shu@comcast.net
Subject: another sample
Date: Sun, 03 Dec 2006 21:21:01 -0500
X-MB-Message-Source: WebUI
MIME-Version: 1.0
From: baspen99@aol.com
X-MB-Message-Type: User
Content-Type: multipart/mixed;
```

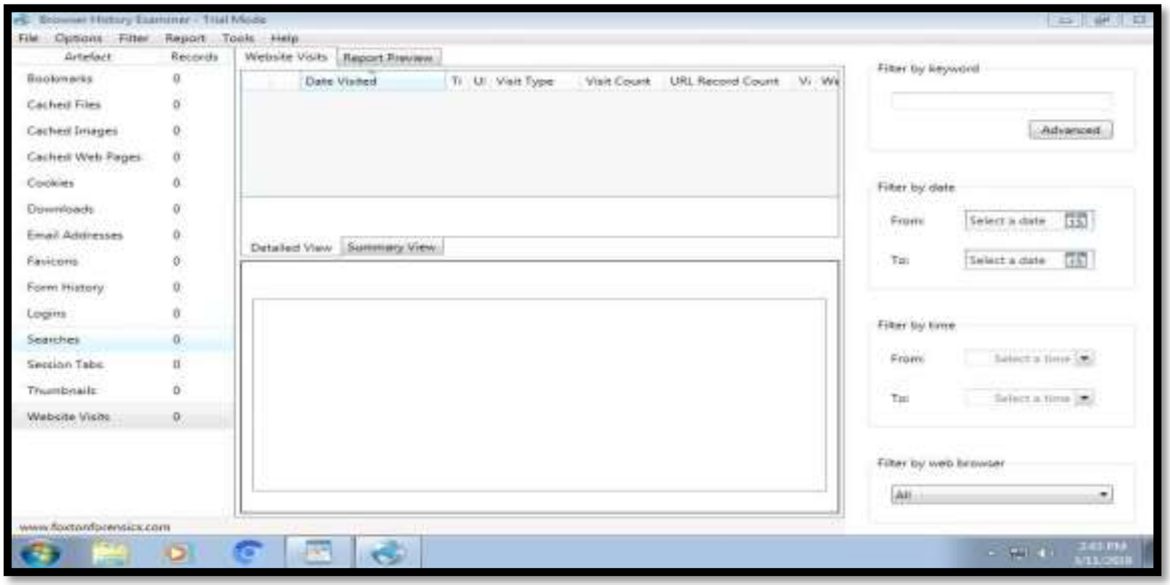
CONCLUSION:- We successfully did Email Forensics using FTK

Practical 9

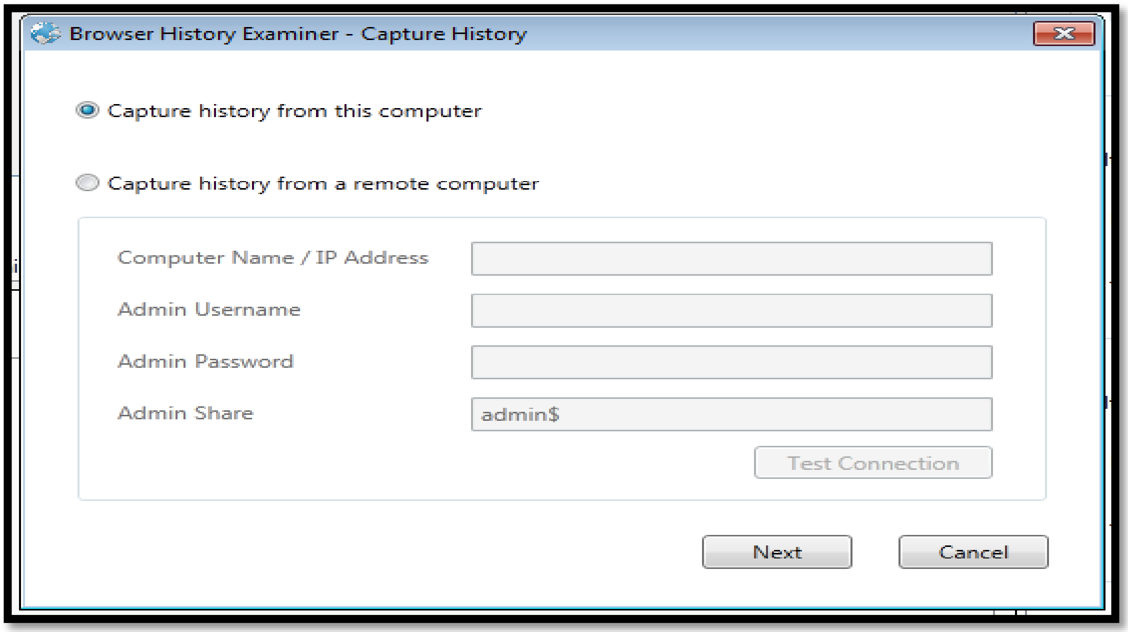
Aim:- Examine Browser History Session Cache files using Browser History Examiner.

You must need a .NET framework and administrative access to the PC.

1. Open Browser History Examiner.



2. Go to File --> Capture History and Select Capture history from this Computer option and click Next.


Browser History Examiner - Capture History

● Capture history from this computer

○ Capture history from a remote computer

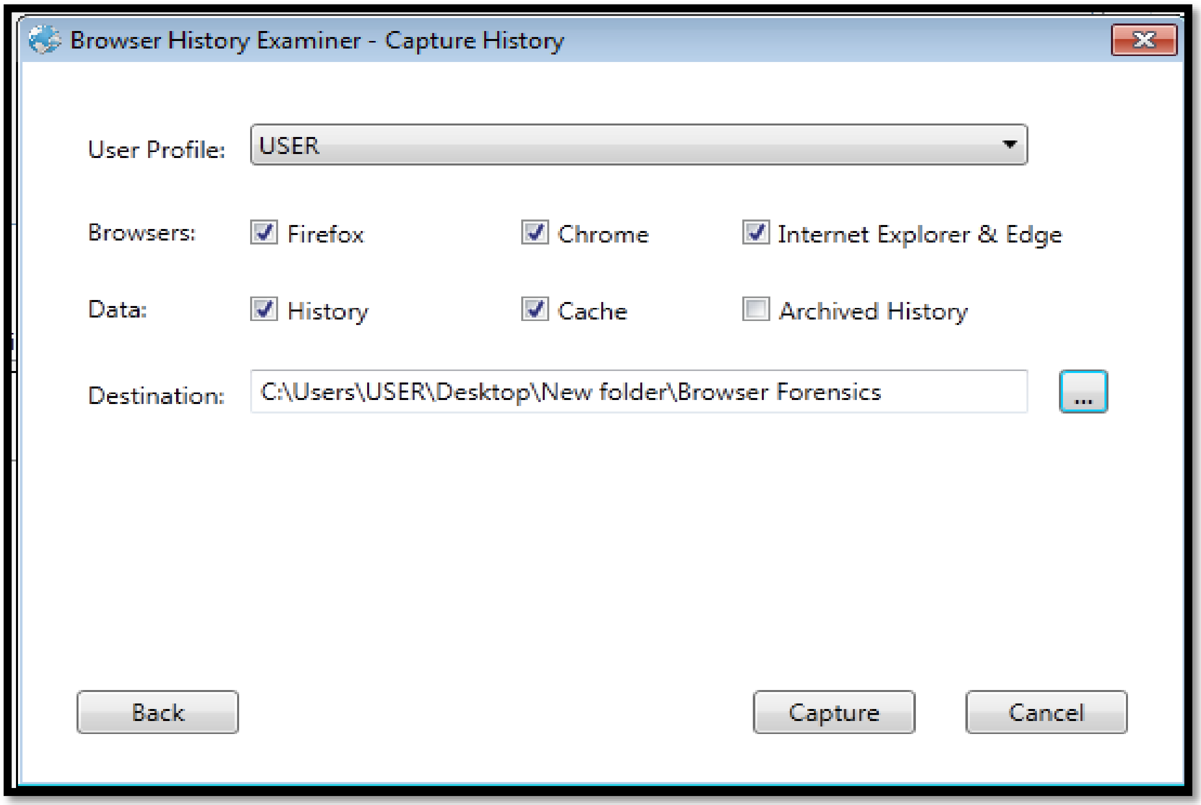
Computer Name / IP Address

Admin Username

Admin Password

Admin Share: admin$

3. Select User Profile, Browser & Data. Also Choose Destination for Results and Click on capture Button.



Browser History Examiner - Capture History

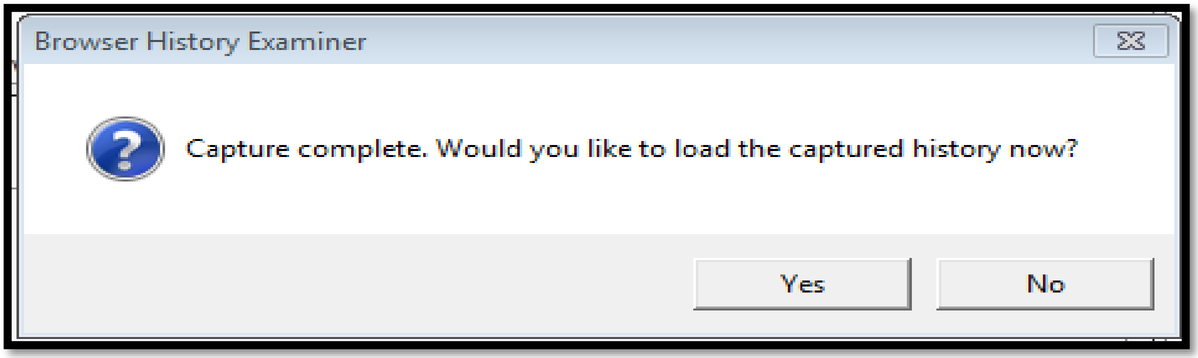
User Profile: USER

Browsers: ☑ Firefox ☑ Chrome ☑ Internet Explorer & Edge

Data: ☑ History ☑ Cache □ Archived History

Destination: C:\Users\USER\Desktop\New folder\Browser Forensics

4. A popup will appear asking to load the history captured as below:-



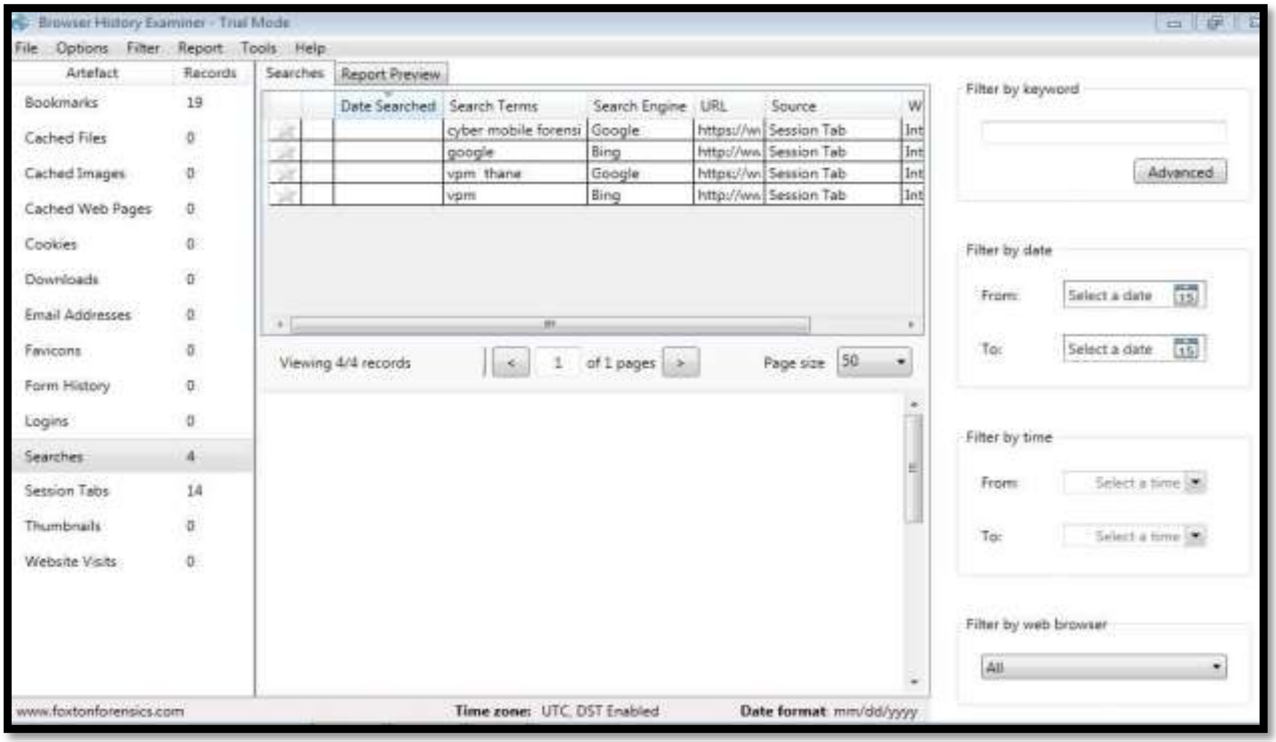
Browser History Examiner

Capture complete. Would you like to load the captured history now?

5. The History will be loaded in Browser History Examiner Window with Different types of Data such as Cache files, Bookmarks, Searches, etc.

The Following Window will appear

Searches ;-



Artefact	Records
Bookmarks	19
Cached Files	0
Cached Images	0
Cached Web Pages	0
Cookies	0
Downloads	0
Email Addresses	0
Favicons	0
Form History	0
Logins	0
Searches	4
Session Tabs	14
Thumbnails	0
Website Visits	0

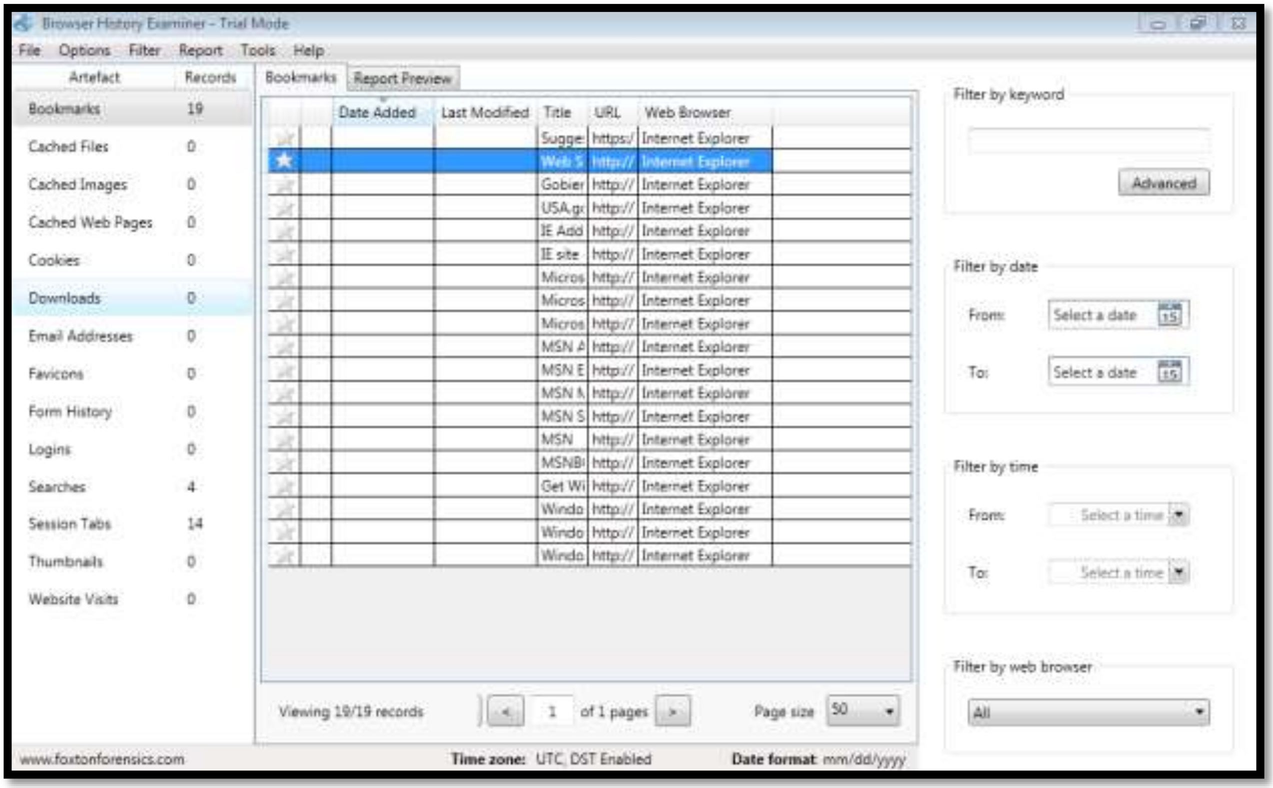
		Date Searched	Search Terms	Search Engine	URL	Source	W
☆			cyber mobile forensi	Google	https://wı	Session Tab	Int
☆			google	Bing	http://ww	Session Tab	Int
☆			vpm thane	Google	https://wı	Session Tab	Int
☆			vpm	Bing	http://ww	Session Tab	Int

Viewing 4/4 records   < 1 of 1 pages >   Page size 50

From: Select a date
To: Select a date
From: Select a time
To: Select a time
All

www.foxtonforensics.com   **Time zone:** UTC, DST Enabled   **Date format** mm/dd/yyyy

Bookmarks:-



Artefact	Records
Bookmarks	19
Cached Files	0
Cached Images	0
Cached Web Pages	0
Cookies	0
Downloads	0
Email Addresses	0
Favicons	0
Form History	0
Logins	0
Searches	4
Session Tabs	14
Thumbnails	0
Website Visits	0

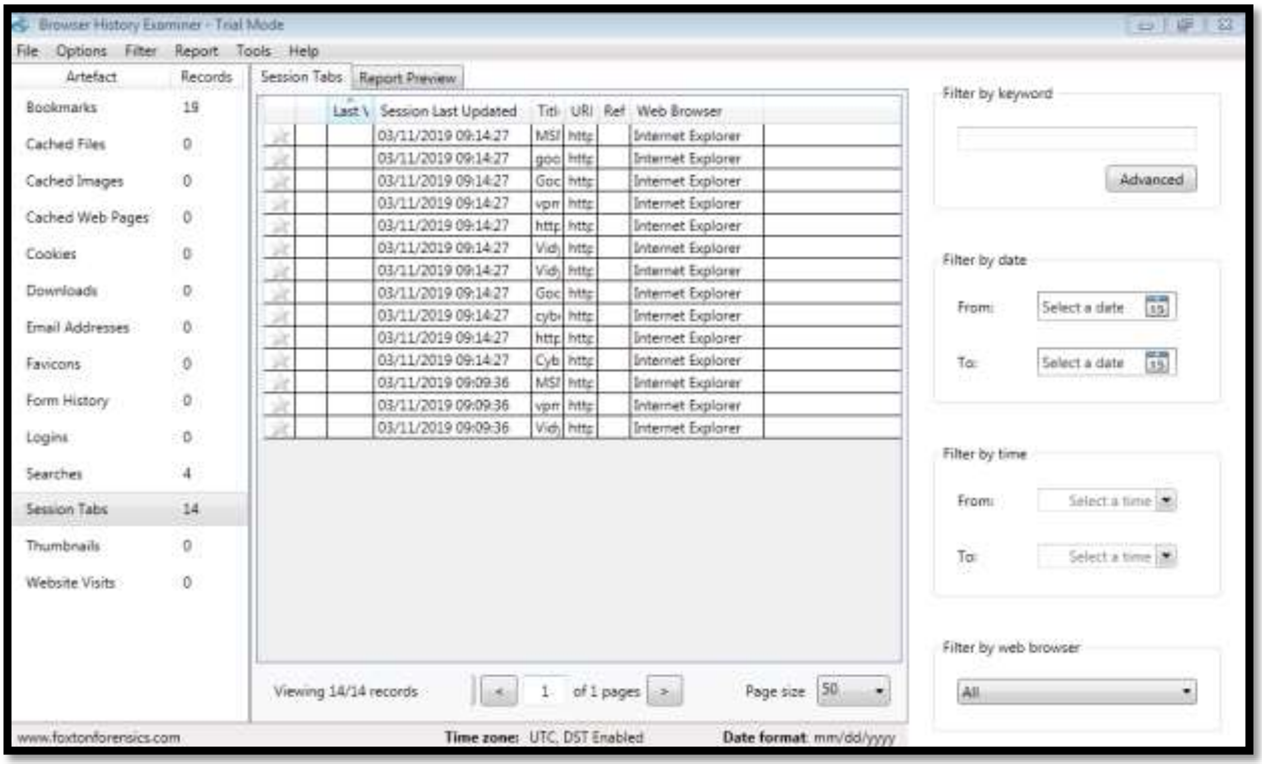
		Date Added	Last Modified	Title	URL	Web Browser
☆				Sugge:	https:/	Internet Explorer
★				Web S	http://	Internet Explorer
☆				Gobier	http://	Internet Explorer
☆				USA.g	http://	Internet Explorer
☆				IE Add	http://	Internet Explorer
☆				IE site	http://	Internet Explorer
☆				Micros	http://	Internet Explorer
☆				Micros	http://	Internet Explorer
☆				Micros	http://	Internet Explorer
☆				MSN A	http://	Internet Explorer
☆				MSN E	http://	Internet Explorer
☆				MSN N	http://	Internet Explorer
☆				MSN S	http://	Internet Explorer
☆				MSN	http://	Internet Explorer
☆				MSNB	http://	Internet Explorer
☆				Get Wi	http://	Internet Explorer
☆				Windo	http://	Internet Explorer
☆				Windo	http://	Internet Explorer
☆				Windo	http://	Internet Explorer

Viewing 19/19 records   < 1 of 1 pages >   Page size 50

From: Select a date
To: Select a date
From: Select a time
To: Select a time
All

www.foxtonforensics.com   **Time zone:** UTC, DST Enabled   **Date format** mm/dd/yyyy

Session Tabs:-



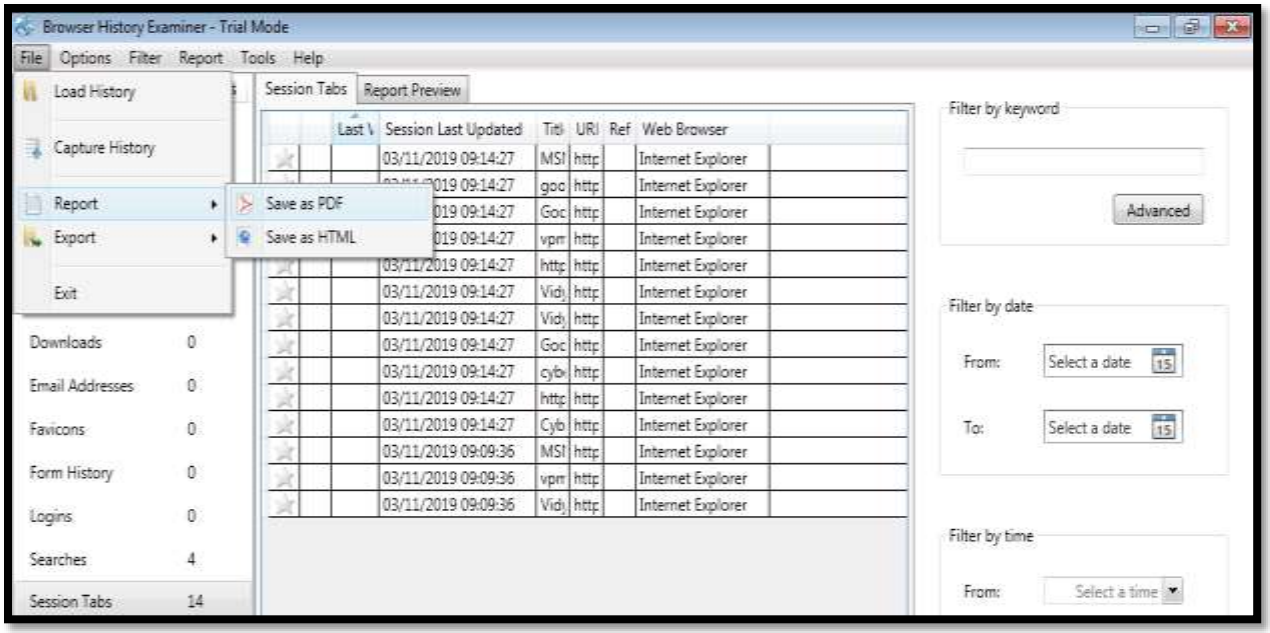
Artefact	Records
Bookmarks	19
Cached Files	0
Cached Images	0
Cached Web Pages	0
Cookies	0
Downloads	0
Email Addresses	0
Favicons	0
Form History	0
Logins	0
Searches	4
Session Tabs	14
Thumbnails	0
Website Visits	0

		Last V	Session Last Updated	Titl	URI	Ref	Web Browser
☆			03/11/2019 09:14:27	MSI	http		Internet Explorer
☆			03/11/2019 09:14:27	goo	http		Internet Explorer
☆			03/11/2019 09:14:27	Goc	http		Internet Explorer
☆			03/11/2019 09:14:27	vpn	http		Internet Explorer
☆			03/11/2019 09:14:27	http	http		Internet Explorer
☆			03/11/2019 09:14:27	Vid	http		Internet Explorer
☆			03/11/2019 09:14:27	Vid	http		Internet Explorer
☆			03/11/2019 09:14:27	Goc	http		Internet Explorer
☆			03/11/2019 09:14:27	cyb	http		Internet Explorer
☆			03/11/2019 09:14:27	http	http		Internet Explorer
☆			03/11/2019 09:14:27	Cyb	http		Internet Explorer
☆			03/11/2019 09:09:36	MSI	http		Internet Explorer
☆			03/11/2019 09:09:36	vpn	http		Internet Explorer
☆			03/11/2019 09:09:36	Vid	http		Internet Explorer

Time zone: UTC, DST Enabled **Date format:** mm/dd/yyyy

6. To Generate Report Of Browser History We go to File → Report.

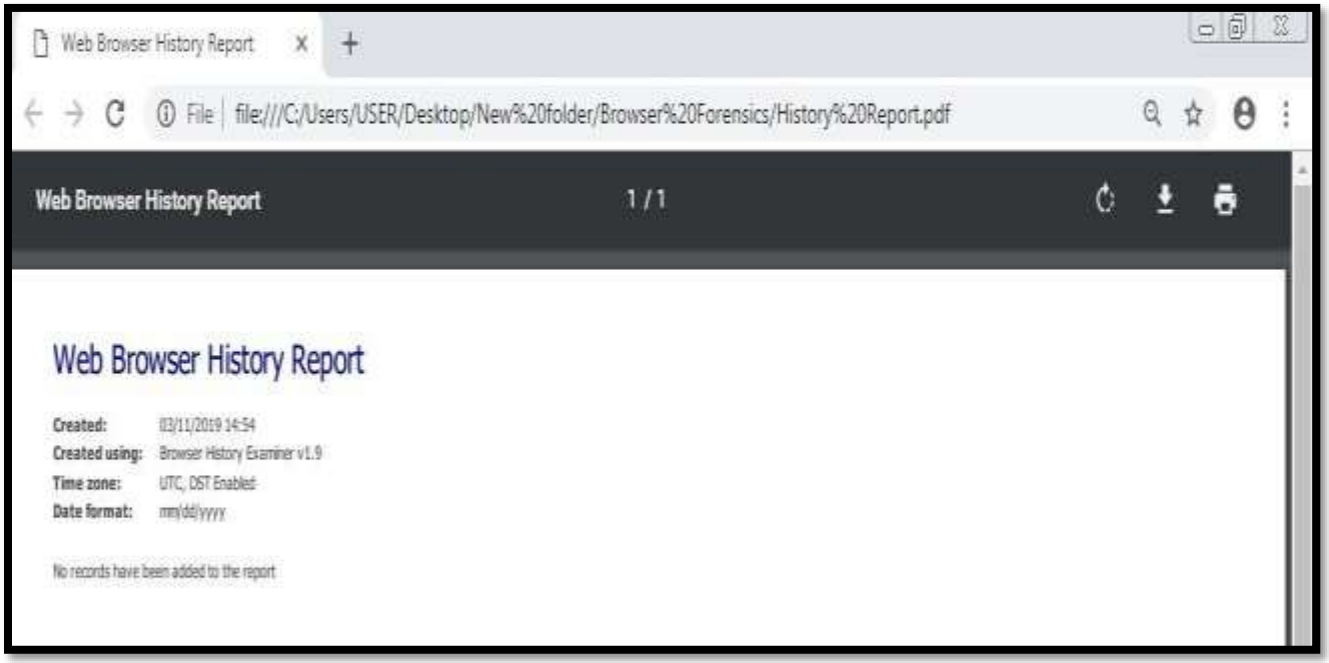
You can choose Both the Operations as a pdf file or as html File.



Downloads	0
Email Addresses	0
Favicons	0
Form History	0
Logins	0
Searches	4
Session Tabs	14

		Last V	Session Last Updated	Titl	URI	Ref	Web Browser
☆			03/11/2019 09:14:27	MSI	http		Internet Explorer
			019 09:14:27	goo	http		Internet Explorer
			019 09:14:27	Goc	http		Internet Explorer
			019 09:14:27	vpn	http		Internet Explorer
☆			03/11/2019 09:14:27	http	http		Internet Explorer
☆			03/11/2019 09:14:27	Vid	http		Internet Explorer
☆			03/11/2019 09:14:27	Vid	http		Internet Explorer
☆			03/11/2019 09:14:27	Goc	http		Internet Explorer
☆			03/11/2019 09:14:27	cyb	http		Internet Explorer
☆			03/11/2019 09:14:27	http	http		Internet Explorer
☆			03/11/2019 09:14:27	Cyb	http		Internet Explorer
☆			03/11/2019 09:09:36	MSI	http		Internet Explorer
☆			03/11/2019 09:09:36	vpn	http		Internet Explorer
☆			03/11/2019 09:09:36	Vid	http		Internet Explorer

7. The Report Will Be Showed As:-

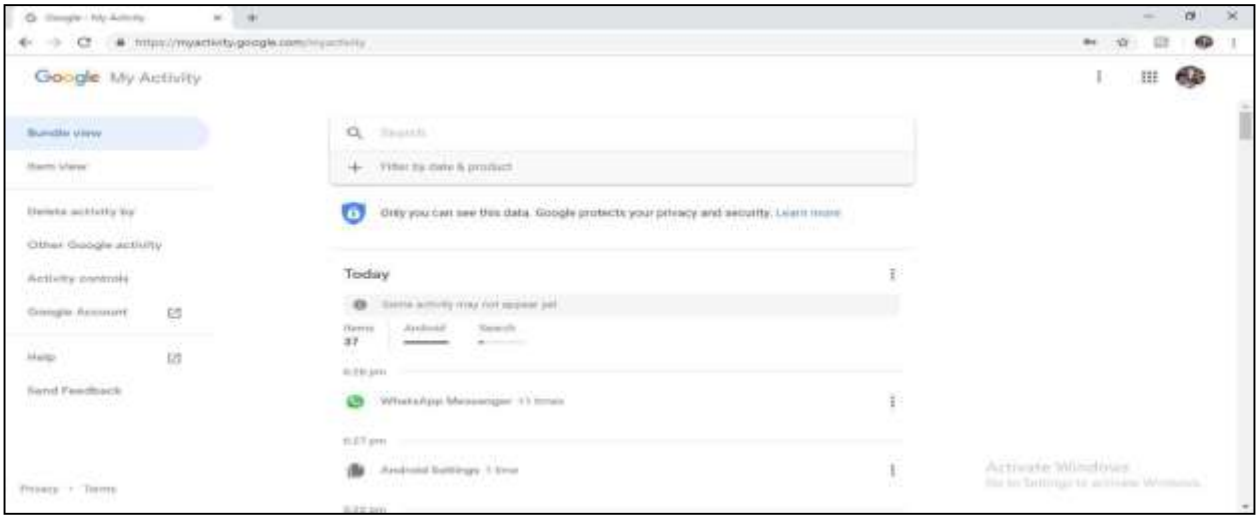

Web Browser History Report
file:///C:/Users/USER/Desktop/New%20folder/Browser%20Forensics/History%20Report.pdf
Web Browser History Report
1 / 1

Web Browser History Report

Created: 03/11/2019 14:54
Created using: Browser History Examiner v1.9
Time zone: UTC, DST Enabled
Date format: mm/dd/yyyy

No records have been added to the report

Browser History using MyActivity

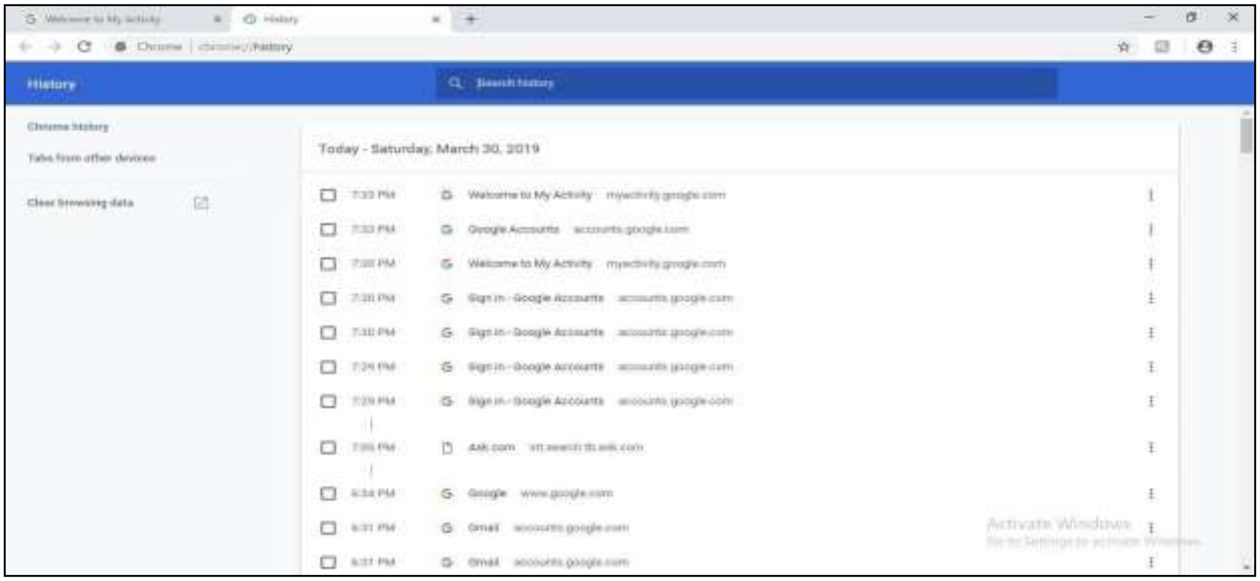


Only you can see this data. Google protects your privacy and security. Learn more

Some activity may not appear yet

WhatsApp Messenger 11 times

Android Settings 1 time



Today - Saturday, March 30, 2019

□ 7:33 PM Welcome to My Activity myactivity.google.com

□ 7:33 PM Google Accounts accounts.google.com

□ 7:32 PM Welcome to My Activity myactivity.google.com

□ 7:30 PM Sign in - Google Accounts accounts.google.com

□ 7:30 PM Sign in - Google Accounts accounts.google.com

□ 7:29 PM Sign in - Google Accounts accounts.google.com

□ 7:29 PM Sign in - Google Accounts accounts.google.com

□ 7:05 PM Ask.com int.search.tb.ask.com

□ 6:34 PM Google www.google.com

□ 6:31 PM Gmail accounts.google.com

□ 6:31 PM Gmail accounts.google.com

CONCLUSION:- We successfully examined Browser History Session Cache files using Browser History Examiner.